



Avid® System Monitor Setup and User's Guide

Version 1.2.1

Legal Notices

Product specifications are subject to change without notice and do not represent a commitment on the part of Avid Technology, Inc.

This product is subject to the terms and conditions of a software license agreement provided with the software. The product may only be used in accordance with the license agreement.

Avid products or portions thereof are protected by one or more of the following United States Patents: 5,267,351; 5,309,528; 5,355,450; 5,396,594; 5,440,348; 5,467,288; 5,513,375; 5,528,310; 5,557,423; 5,577,190; 5,584,006; 5,640,601; 5,644,364; 5,654,737; 5,724,605; 5,726,717; 5,745,637; 5,752,029; 5,754,851; 5,799,150; 5,812,216; 5,828,678; 5,842,014; 5,852,435; 5,986,584; 5,999,406; 6,038,573; 6,069,668; 6,141,007; 6,211,869; 6,532,043; 6,546,190; 6,596,031; 6,747,705; 6,763,523; 6,766,357; 6,847,373; 7,081,900; 7,403,561; 7,433,519; 7,671,871; 7,684,096; D352,278; D372,478; D373,778; D392,267; D392,268; D392,269; D395,291; D396,853; D398,912. Other patents are pending.

Avid products or portions thereof are protected by one or more of the following European Patents: 0506870; 0635188; 0674414; 0752174; 1111910; 1629675. Other patents are pending.

This document is protected under copyright law. An authorized licensee of Interplay Assist may reproduce this publication for the licensee's own use in learning how to use the software. This document may not be reproduced or distributed, in whole or in part, for commercial purposes, such as selling copies of this document or providing support or educational services to others. This document is supplied as a guide for Interplay Assist. Reasonable care has been taken in preparing the information it contains. However, this document may contain omissions, technical inaccuracies, or typographical errors. Avid Technology, Inc. does not accept responsibility of any kind for customers' losses due to the use of this document. Product specifications are subject to change without notice.

Copyright © 2011 Avid Technology, Inc. and its licensors. All rights reserved. Printed in USA.

The following disclaimer is required by Apple Computer, Inc.:

APPLE COMPUTER, INC. MAKES NO WARRANTIES WHATSOEVER, EITHER EXPRESS OR IMPLIED, REGARDING THIS PRODUCT, INCLUDING WARRANTIES WITH RESPECT TO ITS MERCHANTABILITY OR ITS FITNESS FOR ANY PARTICULAR PURPOSE. THE EXCLUSION OF IMPLIED WARRANTIES IS NOT PERMITTED BY SOME STATES. THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. THIS WARRANTY PROVIDES YOU WITH SPECIFIC LEGAL RIGHTS. THERE MAY BE OTHER RIGHTS THAT YOU MAY HAVE WHICH VARY FROM STATE TO STATE.

The following disclaimer is required by Sam Leffler and Silicon Graphics, Inc. for the use of their TIFF library:

Copyright © 1988–1997 Sam Leffler
Copyright © 1991–1997 Silicon Graphics, Inc.

Permission to use, copy, modify, distribute, and sell this software [i.e., the TIFF library] and its documentation for any purpose is hereby granted without fee, provided that (i) the above copyright notices and this permission notice appear in all copies of the software and related documentation, and (ii) the names of Sam Leffler and Silicon Graphics may not be used in any advertising or publicity relating to the software without the specific, prior written permission of Sam Leffler and Silicon Graphics.

THE SOFTWARE IS PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EXPRESS, IMPLIED OR OTHERWISE, INCLUDING WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

IN NO EVENT SHALL SAM LEFFLER OR SILICON GRAPHICS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES OF ANY KIND, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER OR NOT ADVISED OF THE POSSIBILITY OF DAMAGE, AND ON ANY THEORY OF LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

The following disclaimer is required by the Independent JPEG Group:

This software is based in part on the work of the Independent JPEG Group.

This Software may contain components licensed under the following conditions:

Copyright (c) 1989 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Copyright (C) 1989, 1991 by Jef Poskanzer.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. This software is provided "as is" without express or implied warranty.

Copyright 1995, Trinity College Computing Center. Written by David Chappell.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. This software is provided "as is" without express or implied warranty.

Copyright 1996 Daniel Dardailler.

Permission to use, copy, modify, distribute, and sell this software for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Daniel Dardailler not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Daniel Dardailler makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Modifications Copyright 1999 Matt Koss, under the same license as above.

Copyright (c) 1991 by AT&T.

Permission to use, copy, modify, and distribute this software for any purpose without fee is hereby granted, provided that this entire notice is included in all copies of any software which is or includes a copy or modification of this software and in all copies of the supporting documentation for such software.

THIS SOFTWARE IS BEING PROVIDED "AS IS", WITHOUT ANY EXPRESS OR IMPLIED WARRANTY. IN PARTICULAR, NEITHER THE AUTHOR NOR AT&T MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND CONCERNING THE MERCHANTABILITY OF THIS SOFTWARE OR ITS FITNESS FOR ANY PARTICULAR PURPOSE.

This product includes software developed by the University of California, Berkeley and its contributors.

The following disclaimer is required by Nexidia Inc.:

© 2006 Nexidia. All rights reserved.

Manufactured under license from the Georgia Tech Research Corporation, U.S.A. Patent Pending.

The following disclaimer is required by Paradigm Matrix:

Portions of this software licensed from Paradigm Matrix.

The following disclaimer is required by Altura Software, Inc. for the use of its Mac2Win software and Sample Source Code:

©1993–1998 Altura Software, Inc.

The following disclaimer is required by Ultimatte Corporation:

Certain real-time compositing capabilities are provided under a license of such technology from Ultimatte Corporation and are subject to copyright protection.

The following disclaimer is required by 3Prong.com Inc.:

Certain waveform and vector monitoring capabilities are provided under a license from 3Prong.com Inc.

The following disclaimer is required by Interplay Entertainment Corp.:

The "Interplay" name is used with the permission of Interplay Entertainment Corp., which bears no responsibility for Avid products.

This product includes portions of the Alloy Look & Feel software from Incors GmbH.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

© DevelopMentor

This product may include the JCifs library, for which the following notice applies:

JCifs © Copyright 2004, The JCIFS Project, is licensed under LGPL (<http://jcifs.samba.org/>). See the LGPL.txt file in the Third Party Software directory on the installation CD.

Avid Interplay contains components licensed from LavanTech. These components may only be used as part of and in connection with Avid Interplay.

Attn. Government User(s). Restricted Rights Legend

U.S. GOVERNMENT RESTRICTED RIGHTS. This Software and its documentation are “commercial computer software” or “commercial computer software documentation.” In the event that such Software or documentation is acquired by or on behalf of a unit or agency of the U.S. Government, all rights with respect to this Software and documentation are subject to the terms of the License Agreement, pursuant to FAR §12.212(a) and/or DFARS §227.7202-1(a), as applicable.

Trademarks

003, 192 Digital I/O, 192 I/O, 96 I/O, 96i I/O, Adrenaline, AirSpeed, ALEX, Alienbrain, AME, AniMatte, Archive, Archive II, Assistant Station, AudioPages, AudioStation, AutoLoop, AutoSync, Avid, Avid Active, Avid Advanced Response, Avid DNA, Avid DNxcel, Avid DNxHD, Avid DS Assist Station, Avid Liquid, Avid Media Engine, Avid Media Processor, Avid MEDIArry, Avid Mojo, Avid Remote Response, Avid Unity, Avid Unity ISIS, Avid VideoRAID, AvidRAID, AvidShare, AVIDstripe, AVX, Axiom, Beat Detective, Beauty Without The Bandwidth, Beyond Reality, BF Essentials, Bomb Factory, Boom, Bruno, C|24, CaptureManager, ChromaCurve, ChromaWheel, Cineractive Engine, Cineractive Player, Cineractive Viewer, Color Conductor, Command|24, Command|8, Conectiv, Control|24, Cosmonaut Voice, CountDown, d2, d3, DAE, Dazzle, Dazzle Digital Video Creator, D-Command, D-Control, Deko, DekoCast, D-Fi, D-fx, Digi 003, DigiBase, DigiDelivery, Digidesign, Digidesign Audio Engine, Digidesign Development Partners, Digidesign Intelligent Noise Reduction, Digidesign TDM Bus, DigiLink, DigiMeter, DigiPanner, DigiProNet, DigiRack, DigiSerial, DigiSnake, DigiSystem, Digital Choreography, Digital Nonlinear Accelerator, DigiTest, DigiTranslator, DigiWear, DINR, DNxchange, DPP-1, D-Show, DSP Manager, DS-StorageCalc, DV Toolkit, DVD Complete, D-Verb, Eleven, EM, EveryPhase, Expander, ExpertRender, Fader Pack, Fairchild, Fastbreak, Fast Track, Film Cutter, FilmScribe, Flexevent, FluidMotion, Frame Chase, FXDeko, HD Core, HD Process, HDPack, Home-to-Hollywood, HYBRID, HyperControl, HyperSPACE, HyperSPACE HDCAM, iKnowledge, Image Independence, Impact, Improv, iNEWS, iNEWS Assign, iNEWS ControlAir, Instantwrite, Instinct, Intelligent Content Management, Intelligent Digital Actor Technology, IntelliRender, Intelli-Sat, Intelli-sat Broadcasting Recording Manager, InterFX, Interplay, inTONE, Intraframe, iS Expander, ISIS, IsoSync, iS9, iS18, iS23, iS36, ISIS, IsoSync, KeyRig, KeyStudio, LaunchPad, LeaderPlus, LFX, Lightning, Link & Sync, ListSync, LKT-200, Lo-Fi, Luna, MachineControl, Magic Mask, Make Anything Hollywood, make manage move | media, Marquee, MassivePack, Massive Pack Pro, M-Audio, M-Audio Micro, Maxim, Mbox, Media Composer, MediaDock, MediaDock Shuttle, MediaFlow, MediaLog, MediaMatch, MediaMix, Media Reader, Media Recorder, MEDIArry, MediaServer, MediaShare, MetaFuze, MetaSync, MicroTrack, MIDI I/O, Midiman, Mix Rack, MixLab, Moviebox, Moviestar, MultiShell, NaturalMatch, NewsCutter, NewsView, Nitris, NL3D, NLP, Nova, NRV-10 interFX, NSDOS, NSWIN, Octane, OMF, OMF Interchange, OMM, OnDVD, Open Media Framework, Open Media Management, Ozone, Ozonic, Painterly Effects, Palladium, Personal Q, PET, Pinnacle, Pinnacle DistanTV, Pinnacle GenieBox, Pinnacle HomeMusic, Pinnacle MediaSuite, Pinnacle Mobile Media, Pinnacle Scorefitter, Pinnacle Studio, Pinnacle Studio MovieBoard, Pinnacle Systems, Pinnacle VideoSpin, Podcast Factory, PowerSwap, PRE, ProControl, ProEncode, Profiler, Pro Tools|HD, Pro Tools LE, Pro Tools M-Powered, Pro Transfer, Pro Tools, QuickPunch, QuietDrive, Realtime Motion Synthesis, Recti-Fi, Reel Tape Delay, Reel Tape Flanger, Reel Tape Saturation, Reprise, Res Rocket Surfer, Reso, RetroLoop, Reverb One, ReVibe, Revolution, rS9, rS18, RTAS, Salesview, Sci-Fi, Scorch, Scorefitter, ScriptSync, SecureProductionEnvironment, Serv|LT, Serv|GT, Session, Shape-to-Shape, ShuttleCase, Sibelius, SIDON, SimulPlay, SimulRecord, Slightly Rude Compressor, Smack!, Soft SampleCell, Soft-Clip Limiter, Solaris, SoundReplacer, SPACE, SPACESHift, SpectraGraph, SpectraMatte, SteadyGlide, Streamfactory, Streamgenie, StreamRAID, Strike, Structure, Studiophile, SubCap, Sundance Digital, Sundance, SurroundScope, Symphony, SYNC HD, Synchronic, SynchroScope, SYNC I/O, Syntax, TDM FlexCable, TechFlix, Tel-Ray, Thunder, Titansync, Titan, TL Aggro, TL AutoPan, TL Drum Rehab, TL Everyphase, TL Fauxlder, TL In Tune, TL MasterMeter, TL Metro, TL Space, TL Utilities, tools for storytellers, Torq, Torq Xponent, Transfuser, Transit, TransJammer, Trigger Finger, Trillium Lane Labs, TruTouch, UnityRAID, Vari-Fi, Velvet, Video the Web Way, VideoRAID, VideoSPACE, VideoSpin, VTEM, Work-N-Play, Xdeck, X-Form, Xmon, XPAND!, Xponent, X-Session, and X-Session Pro are either registered trademarks or trademarks of Avid Technology, Inc. in the United States and/or other countries.

Avid System Monitor Setup and User's Guide • 0130-30477-01 Rev F • January 2012 • Created 1/30/12 • This document is distributed by Avid in online (electronic) form only, and is not available for purchase in printed form.

Contents

	Revision History	11
	Symbols and Conventions	12
	If You Need Help	12
Chapter 1	Overview and System Requirements	15
	What is Avid System Monitor and OpenNMS?	15
	What is a MIB?	16
	Setting Expectations - Benefits and Limitations	17
	An Overview of System Monitoring	17
	Overview of Avid System Monitor Data Collection	18
	An Example Monitoring Workflow for Automatic Discovery	19
	Systems Monitored by Avid System Monitor	21
	Avid System Monitor Server System Requirements	24
	Installation Overview	24
	What to Bring to an Installation	24
	Software Installation Checklist	25
	Software Installation and Configuration on the OpenNMS Server and Individual Nodes	25
	Configuration From Within the OpenNMS Interface	27
	Configuration Files	28
	Backing Up the Avid System Monitor Files	30
Chapter 2	Getting Started with OpenNMS	31
	New for Avid System Monitor v1.2.1	31
	New Features for Avid System Monitor	31
	New for OpenNMS v1.8.10	32
	Changes to Provisioning Groups	32
	New Location for Provisioning Group Templates	32
	Changes to the Provisioning Groups User Interface	32

	Changes to ISIS Client Service Name for ISIS v2.3 and Later.	34
	Terminology	34
	The OpenNMS Main Page	35
	The Node List.	36
	The Dashboard and Surveillance View	38
	Resource Graphs and Reports.	39
	The Map Page	41
	The Search Page	42
Chapter 3	Installing Software on the Avid System Monitor Server.	43
	Upgrading from Avid System Monitor v1.1.1	43
	Preparing the OpenNMS Server	43
	Installing the Basic OpenNMS Server Software.	45
	Restarting or Stopping OpenNMS	51
	Uninstalling Avid System Monitor.	52
	Configuring Time Sync on the Monitoring Server.	52
Chapter 4	Configuring Monitored Nodes.	55
	Configuring the Windows SNMP Agent	55
	Installing and Configuring the Windows SNMP Agent.	55
	Installing the SNMP Services	56
	Configuring the Microsoft SNMP Agent	58
	Customizing the SNMP Community String Value	62
	Configuring the Interplay Engine	63
	Adding an SNMP User to the Interplay Database.	65
	Using Provisioning Groups to Add an Interplay Engine to OpenNMS	67
	Configuring an Interplay Stream Server.	67
	Configuring the ISIS System Director.	68
	Installing the ISIS SNMP Agent.	68
	Configuring ISIS System Directors	68
	Identifying a 64-bit Server.	70
	Configuring a Media Indexer	70
	Selecting the Software Version of the Media Indexer	70
	Configuring Additional Servers with the Monitoring Gateway	72
	Installing the Avid Monitoring Gateway Service	73

	Monitoring Gateway in the Service Configuration Tool	74
	Generating SNMP Traps from a Network Switch	74
	Configuring a Cisco Switch	74
	Configuring a Foundry Switch	76
	Configuring a Force10 Switch	78
	Using Add Interface to Add a Network Switch to OpenNMS	79
	Configuring Data Collection for a Network Switch	79
Chapter 5	Working with Provisioning Groups	83
	Overview of Provisioning Groups	83
	Determining Which Provisioning Group Template to Use	83
	Configuring a Standalone Interplay Engine.	84
	Critical Alarms When First Adding an Interplay Engine	88
	Configuring Cluster Systems.	88
	Using Provisioning Groups to Configure an Interplay Engine Cluster	90
	Interplay Engines and ISIS v2.3 and v2.4	94
	Replacing the Service Before You Configure the Interplay Engine Provisioning Group	96
	Replacing the Service After You Configure the Provisioning Group	97
	Using Provisioning Groups to Configure an ISIS 7000 System Director.	101
	Configuring an Interplay Stream Server	102
	Defining Nodes with Basic Up/Down Status	103
	Creating New Provisioning Groups.	106
Chapter 6	Configuring Discovery and the Dashboard	109
	Methods for Discovering Systems to be Monitored.	110
	Provisioning Groups versus Add Interface.	111
	Configuring Discovery Using Add Interface	111
	Using the Add Interface Command to Add Nodes	112
	Deleting the Default Discovery Range	113
	Configuring the Dashboard	113
	Determine the Category Names for the Site	114
	Delete the Default Surveillance Categories and Add New Ones	114
	Trouble Shooting	117
	Adding Nodes to Surveillance Categories	117

	Naming the Discovered Nodes	119
Chapter 7	Working With Notifications and Maps	121
	Working with Email Notifications	121
	Turning Notifications On and Off Globally	121
	Preparing the OpenNMS Server for Email Notification	122
	Assigning the Admin Email Account	123
	Turning on Notifications and Specifying a Target Email Address	125
	Adding Useful Text to an Email Notification	129
	Sending Notifications to An External Monitoring System	129
	Setting Up the Receiving SNMP Monitoring System	130
	Configuring OpenNMS to Send Traps to the Monitoring System	131
	Defining Notifications to Send to an External Monitoring System	133
	Known Problem with Editing an Existing Trap Notification	137
	Working with Maps	138
	Turning on the Map Feature	138
	Showing Switch Connectivity	139
	Installing the Adobe SVG Viewer	139
	Known Problems with the Map Feature	140
	Creating a New Map	140
	Adding a Background Graphic	143
	Opening an Existing Map and Viewing Node Status	144
Chapter 8	Working with OpenNMS	147
	Changing Threshold Values	148
	Known Problems with Notifications for the Interplay Engine and Stream Server	151
	Changes for the Stream Server	152
	Changing the Text Notifications for the Stream Server	156
	Number of Objects in the Interplay Database	157
	Handle Count and Thread Count	157
	Troubleshooting	157
	Examine the Home Page and Dashboard	157
	Examine the Resource Graphs	159
	Solving Configuration Problems	160

Fixing a Problem When Provisioning Groups Nodes Don't Appear	160
Modifying Notifications from ISIS	161
Working with Resource Graphs	163
Displaying Resource Graphs	163
Notes About the Graphs.	166
Creating Reports	167
Removing Discovered Services from a Node	173
Working with Alarms	175
Acknowledging Alarms.	181
Running the Avid System Monitor Upgrade Utility	186
Setting the Path Environment Variable for Java.	187
Correcting Links to the OpenNMS Home Page After the Upgrade	188
Modifying Provisioning Groups after the Upgrade	188
Backing Up and Restoring Avid System Monitor	192
To Perform a Complete Backup of Avid System Monitor.	192
Backing Up and Restoring the PostgreSQL Database.	192
Backing Up the PostgreSQL Database	192
Restoring the PostgreSQL Database	194
Restoring an Avid System Monitor Backup.	198

Using This Guide

This guide contains an overview of Avid System Monitor application and also contains the task-oriented instructions, and conceptual information you need to install, configure, and use Avid System Monitor. This guide is intended for all Avid System Monitor users, from installation, to beginning and advanced users.

Revision History

Date Revised	Changes Made
01/30/2012	Added or updated the following: • “Known Problems with Notifications for the Interplay Engine and Stream Server” on page 151 • “Interplay Engines and ISIS v2.3 and v2.4” on page 94 • “Installing the Avid Monitoring Gateway Service” on page 73 • “Changing Threshold Values” on page 148
11/4/2011	Updated the following: • “Configuring ISIS System Directors” on page 68 • “Changes for the Stream Server” on page 152 • “Running the Avid System Monitor Upgrade Utility” on page 186
8/30/2011	Updated for Avid System Monitor v1.2.1.

Symbols and Conventions

Avid documentation uses the following symbols and conventions:

Symbol or Convention	Meaning or Action
	A note provides important related information, reminders, recommendations, and strong suggestions.
	A caution means that a specific action you take could cause harm to your computer or cause you to lose data.
	A warning describes an action that could cause you physical harm. Follow the guidelines in this document or on the unit itself when handling electrical equipment.
>	This symbol indicates menu commands (and subcommands) in the order you select them. For example, File > Import means to open the File menu and then select the Import command.
▶	This symbol indicates a single-step procedure. Multiple arrows in a list indicate that you perform one of the actions listed.
Bold font	Bold font is primarily used in task instructions to identify user interface items and keyboard sequences.
<i>Italic font</i>	Italic font is used to emphasize certain words and to indicate variables.
Courier Bold font	Courier Bold font identifies text that you type.
Ctrl+key or mouse action	Press and hold the first key while you press the last key or perform the mouse action. For example, Command+Option+C or Ctrl+drag.

If You Need Help

If you are having trouble using your Avid product:

1. Retry the action, carefully following the instructions given for that task in this guide. It is especially important to check each step of your workflow.
2. Check the latest information that might have become available after the documentation was published:
 - If the latest information for your Avid product is provided as printed release notes, they ship with your application and are also available online.

If the latest information for your Avid product is provided as a ReadMe file, it is supplied on your Avid installation CD or DVD as a PDF document (README_*product*.pdf) and is also available online.

You should always check online for the most up-to-date release notes or ReadMe because the online version is updated whenever new information becomes available. To view these online versions, select ReadMe from the Help menu, or visit the Knowledge Base at www.avid.com/readme.

3. Check the documentation that came with your Avid application or your hardware for maintenance or hardware-related issues.
4. Visit the online Knowledge Base at www.avid.com/online support. Online services are available 24 hours per day, 7 days per week. Search this online Knowledge Base to find answers, to view error messages, to access troubleshooting tips, to download updates, and to read or join online message-board discussions.

1 Overview and System Requirements

This chapter provides a brief overview of the main components that make up the Avid System Monitor.

- [What is Avid System Monitor and OpenNMS?](#)
- [What is a MIB?](#)
- [Setting Expectations - Benefits and Limitations](#)
- [An Overview of System Monitoring](#)
- [Avid System Monitor Server System Requirements](#)
- [Installation Overview](#)
- [Backing Up the Avid System Monitor Files](#)

What is Avid System Monitor and OpenNMS?

Avid System Monitor is implemented via OpenNMS (Open Source Network Management System). OpenNMS is an enterprise-grade network monitoring platform developed under the open source software model. It consists of a community-supported, open-source project as well as an organization offering commercial services, training and support.

OpenNMS uses a web-based GUI to present the following network management tools:

- Service polling - determining service availability and latency, and reporting on the results.
- Data collection - collecting, storing and reporting on data collected from nodes via protocols including SNMP, JMX, HTTP, Windows Management Instrumentation, and NSClient.
- Thresholding - evaluating polled latency data or collected performance data against configurable thresholds, creating events when these are exceeded or rearmed.
- Event management - receiving events, both internal and external, including SNMP traps.
- Alarms and automations - reducing events according to a reduction key and scripting automated actions centered around alarms.
- Notifications - sending notices regarding noteworthy events via e-mail, XMPP, or other means.

1 Overview and System Requirements

For additional information on OpenNMS, see their web page:

<http://www.opennms.org/>

This document describes the installation and configuration techniques used to run the Avid System Monitor application in an Interplay environment.

Throughout this document, the term OpenNMS is used to describe specific information such as the OpenNMS software installation and the location of configuration file folders. The term Avid System Monitor is used to describe Avid's implementation of OpenNMS. For the purposes of installation and configuration, the two terms are often interchangeable.

What is a MIB?

The term MIB stands for Management Information Base. A MIB is a file that defines the set of variables used by SNMP (Simple Network Management Protocol) to monitor components on a network. Many components, such as network switches, come with their own MIB tables that define the features of the switch that can be monitored. A switch or other network component sends information to a monitoring agent via SNMP traps. You configure the SNMP agent service on the network component to send traps to particular IP addresses such as the IP address of the server running OpenNMS. The SNMP agent monitors the system it is running on and when it identifies a condition corresponding to a value in the MIB table, it automatically sends a trap to the monitoring system.

OpenNMS automatically recognizes a number of standard MIB tables such as tables for Foundry and Cisco network switches. OpenNMS also has the ability to import MIB tables so that other network components can also be monitored. For example, the Interplay SNMP agent installer contains MIB tables for the Interplay Engine and Interplay Stream Server. These MIB tables have been imported into Avid's implementation of OpenNMS so that those systems can be monitored via SNMP traps. In future releases, Avid will import additional MIB tables (including third party MIB tables) into its OpenNMS implementation.

Besides responding to traps sent by an SNMP agent, OpenNMS also uses a polling technique to poll the SNMP agent on a regular basis, usually every 5 minutes. It compares the polling information and the traps against pre-configured thresholds. If a threshold value is exceeded, OpenNMS creates an event that appears in the interface and is stored in the PostgreSQL database used by OpenNMS. The event can in turn generate alarms that appear in the interface and notifications that can be sent via email.

Setting Expectations - Benefits and Limitations

The Avid System Monitor system has a lot of potential for monitoring and reporting on the state of a system such as an Interplay environment. At this early stage in the development of Avid System Monitor, it is important to set expectations about what you can expect from the system.

Benefits of the Avid Monitoring Solution

- It can help you identify problems in your system as they are occurring.
- It provides a single tool for monitoring all necessary components of the system, including Avid equipment, network infrastructure, and 3rd party devices.
- Collects performance data over time for graphical trend analysis.
- It is a tool that will continually evolve to identify potential issues within a system as we gain knowledge about how to solve problems at customer sites.
- It provides visibility into the specific state of the Avid system components at a given point in time. It also provides flexibility for customers to refine and fine tune the tool's outputs once the basic functions are mastered.

Current Limitations of the Avid Monitoring Solution

- It is not a replacement for a trained administrator actively monitoring the proper functioning of their system.
- It is not a tool that will identify all potential problems that would affect workflows. It identifies common problems but there are other potential problems that it cannot yet identify.
- It is not a tool that can be used to determine usage statistics. In other words, it is not a reliable source to determine and base business models on, such as billing.
- It is not able to accurately model service-level agreements (SLA) or Service Level objectives (SLO) for the system components.

An Overview of System Monitoring

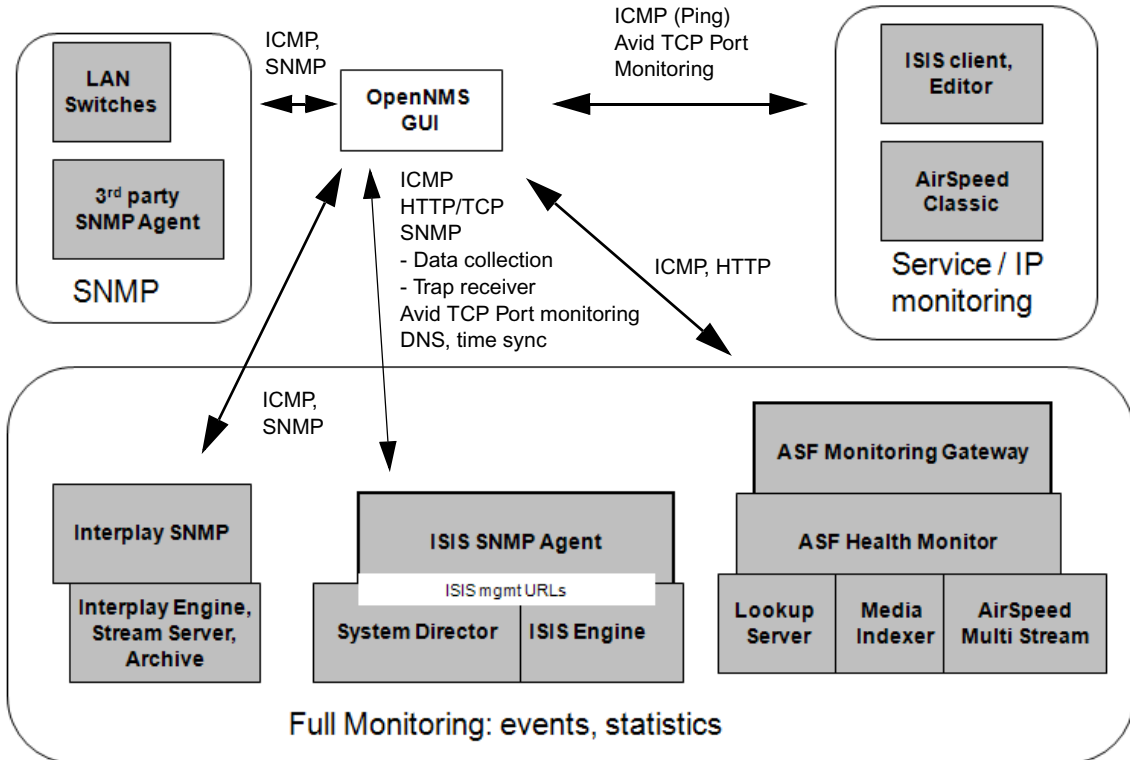
This section covers the following topics:

- [Overview of Avid System Monitor Data Collection](#)
- [An Example Monitoring Workflow for Automatic Discovery](#)
- [Systems Monitored by Avid System Monitor](#)

Overview of Avid System Monitor Data Collection

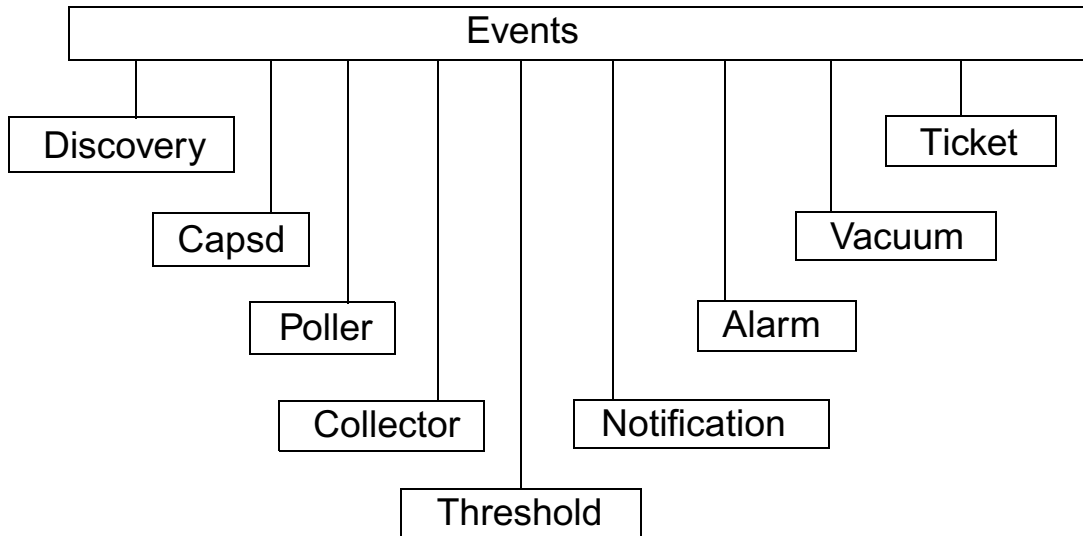
The following illustration shows how OpenNMS interacts with the various elements of the Interplay environment.

- Monitoring Gateway uses HTTP data collection to collect information from specific systems that are running the Avid Service Framework Health Monitor.
- A number of devices are configured just for up/down status. OpenNMS uses ping and ICMP to check the availability and response time of these devices.
- The ISIS Engine, Interplay Engine, Archive Engine, and Interplay Stream Server have their own custom SNMP agents that send SNMP data to OpenNMS.
- You can also configure LAN switches such as Cisco and Foundry switches to send SNMP data to OpenNMS.



An Example Monitoring Workflow for Automatic Discovery

Systems that are monitored by OpenNMS are called nodes. Monitoring can range from a simple Ping (to monitor up/down status) to full service monitoring and statistics gathering. The following illustration shows the inter process communication within the OpenNMS application during node monitoring. A typical workflow moves from left to right.



OpenNMS runs the discovery process every 24 hours. Systems that are configured for discovery are examined by the Capsd process at that time. This means that additional services that are installed on the node will be picked up on the next automatic discovery.

Note that only systems that are configured for automatic discovery use the Discovery portion of this workflow. This includes systems that are configured via Add Interface command: Avid Media Indexer, Lookup Service, Interplay Capture. On systems configured via Provisioning Groups, OpenNMS looks for specific services as defined in the provisioning group template. For additional information, see [“Overview of Provisioning Groups” on page 83](#).

The following describes the basic workflow.

- The system administrator uses the OpenNMS interface to specify the IP addresses of systems to monitor. For example, the Add Interface command identifies a system and initiates discovery.
- The Discovery process pings those IP addresses and determines whether there is an SNMP agent on each of the machines (nodes) in the range.

1 Overview and System Requirements

- The Capsd (capabilities) process is defined to look for a set of specific services on each discovered node. It checks whether those services exist on the node and registers with OpenNMS if the services exist. For example, Capsd checks whether the various Interplay Service Framework services are running on the node.

The following illustration shows an Interplay Engine with a number of services running, including the Interplay Engine service, the ISIS client, and the Windows Cluster service.

Home / Search / Node
Node: a51-wg1-eng1.global.avidww.com

[View Events](#) [View Alarms](#) [Asset Info](#) [Site Status](#) [Resource Graphs](#) [Rescan](#) [Admin](#) [Update SNMP](#)

General (Status: Active)
View Node Link Detailed Info

Availability

Availability (last 24 hours)		
10.105.224.4	Overall	100.000%
	AvidISISClient	100.000%
	AvidInterplayEngine	100.000%
	ICMP	100.000%
	SNMP	100.000%
	StrafePing	100.000%
	Win32AvidFosFS	100.000%
	Win32AvidUnityISISClientAgent	100.000%
	Win32ClusterService	100.000%
	Win32NetLogon	100.000%
	Win32Server	100.000%
	Win32Time	100.000%

Notification
You: Outstanding: (Check)
You: Acknowledged: (Check)

Recent Events

☐	280	8/20/10 13:41:20
☐	279	8/20/10 13:41:20
☐	278	8/20/10 13:41:20
☐	277	8/20/10 13:41:20
☐	276	8/20/10 13:41:20

M

Recent Outages
There have been no outages on

- Now that OpenNMS knows the service is present on the node, it uses the Poller process to periodically check whether the service is running (whether the service is up). For example, by default the Poller checks every five minutes whether the SNMP process is up on the node.
- The Collector process is configured to collect data from the node depending on which services are present. For example, if the node is a Cisco router, it will collect Cisco-specific data. If the Avid Interplay Media Indexer process is present, it will collect data such as the number of media files monitored and the amount of free memory on the Media Indexer.

- As the data is collected, the Threshold process tests for threshold values. If a threshold is exceeded it will generate an event. The system administrator can configure how OpenNMS responds to these events.
- If the Poller determines that the service is not responding, it generates a Node Lost Service event. at this point the system checks the Notification configuration to determine whether any notifications should be sent when this service is down. For example, you can configure notifications to generate email containing the event data.
- An Alarm is also generated at this point. The Alarm is displayed in the OpenNMS UI. An administrator can use the UI to acknowledge the alarm. The Vacuum process cleans out the alarms once they are acknowledged.
- You can configure OpenNMS to act depending on whether the Alarm is acknowledged. For example, if an alarm is not acknowledged within 10 minutes it can be escalated to a major alarm. If a major alarm is not acknowledged within 20 minutes it can be escalated to a critical alarm which can cause a Ticket event. You can configure ticket events to generate emails or even generate phone calls or pager calls.

When using notifications or alarms you can also configure the system to wait a specific number of minutes and check whether a node down event is followed by a corresponding node up event. In that case the system can avoid sending out needless notifications if there was just a temporary problem with the network.

Systems Monitored by Avid System Monitor

The following table describes the systems that Avid System Monitor monitors and the components on the system that are monitored.

System to Monitor	Items to Monitor
Network Switches	Network infrastructure Zone 2 switches such as Cisco and Foundry switches come with installed MIB tables that are accessible via SNMP traps. You can log onto a switch and configure it to send traps to the Avid System Monitor system. The following are examples of what can be monitored: • SNMP: Link Up, Link down • Network: spanning tree topology changes and bandwidth utilization. • System: memory utilization and processor utilization • Thermal: max temperature exceeded • Cisco: configuration changes • Foundry: startup config change, running config change, telnet login or logout

1 Overview and System Requirements

System to Monitor	Items to Monitor
Interplay Engine	Time to perform login - should be below 15 seconds: indicates engine slowness or network connectivity problems Number of journal files - should be below 50: indicates that journal integration is not running Number of deletes - allows you to monitor the number of deletes during 5 minute polling intervals. Excessive deletes during normal production time can affect system performance Number of loaded objects/number of total objects - should be above 30%: indicates engine cache warm-up causing slowness Backup running flag - backups should usually not be performed during production time
Interplay Stream Server	Check the availability of the Streaming server share (WG_Stream\$) Uptime of the service and CPU load Number of current connections and the bandwidth of current connections Number of client connections and the current number of streaming sessions
Avid ISIS 7000 Avid ISIS 5000	Starting at Avid System Monitor v1.1, you can monitor both ISIS 7000 and ISIS 5000 System Directors. The following are some of the areas you can monitor. Temperature and presence of components such as switches, storage elements, and power supplies. Workspace usage thresholds. For example, an Admin can enable warning and error thresholds. If you can set the workspace threshold to 90%, ISIS will generate an error event when a workspace reaches 90% full These messages can be sent to OpenNMS via SNMP traps. Disk health issues such as disk failed or disk performance degraded based on continuous monitoring. Server failover notifications. For example, on a failover system you are notified when the system fails over to the other node. Metadata problems. For example: if there is a problem opening a metadata file or if the metadata in a file seems out of date
Media Indexer	Number of unique media files being monitored by a Media Indexer in the HAG approaching or exceeding recommended limits. Different time on each of the machines in the WG: Can be the cause of lost ISIS notifications (see above). Number of handshaker errors growing

System to Monitor	Items to Monitor
AirSpeed Multi Stream	Memory Usage Application status (warning if application is not responding) Percentage free disk space (warnings if below 20% and 10%) Number of successful transfers and number of failed transfers Genlock status (warning if system is not using Genlock) Power supply status (warning that a power supply has failed or may be unplugged) Temperature status (OK or warning based on consolidated values from Health Monitor) Fan speed status (similar to temperature status)
Avid Interplay Capture	Handle Count - should be below 18000^a Thread Count - should be below 3000 Number of channels and channel pools - each should be less than 50. Number of simultaneous recordings - should be less than 5000 Redundancy weight and redundancy group size should be greater than 1.
Avid Service Framework Lookup Service	Handle Count - should be below 5000 Thread Count - should be below 500 Events In Queue - should be less than 50 Check that a process is bound to port 4160 - confirms that the LUS process is running Memory Usage - should be below 200MB

a. For additional information, see [“Handle Count and Thread Count” on page 157](#).

Avid System Monitor Server System Requirements

The following table lists the basic requirements for the server that runs the Avid System Monitor application.

Category	Description
Operating System	Windows Server 2003 or Windows Server 2008. Windows XP is not recommended because it has a limit on the number of TCP connections that can be used.  <i>When using Windows Server 2008 64-bit, at least 4 GB RAM is required.</i>
Processor	A 2 GHz processor or better. Avid System Monitor can also take advantage of multiple processors.
Memory	A minimum of 2 GB of RAM. The Avid System Monitor Java Virtual Machine benefits from large amounts of memory.

At this time, virtual machines are not recommended for performance reasons.

 *On a 64-bit system, install the 32-bit version of OpenNMS, Java, and PostgreSQL. The 64-bit version of OpenNMS has not been qualified with Avid System Monitor.*

Installation Overview

This section provides an overview of the software that is installed and configured on the Avid System Monitor server and on other systems in the Interplay environment.

What to Bring to an Installation

The Avid System Monitor server software is qualified on Intel SR2400 and SR2500 systems. SR2500 servers are preferred but you can use a re-purposed SR2400 if it meets the hardware qualifications. See [“Avid System Monitor Server System Requirements” on page 24](#). The following lists the items that you may find useful at an installation.

- Interplay Engine Recovery DVD for SR2400 and SR2500 - use these DVDs to initialize a server that will be repurposed as an Avid System Monitor server.
- On an AS3000, use the same system image as an Interplay Engine, Windows Server 2008 Standard x64, and install the 32-bit version of OpenNMS.

- Avid System Monitor installer.
- Bring the following DVDs in case you need to install the Intel SNMP agent on a node:
 - Windows XP Professional
 - Windows 2003 Server Standard (32-bit)
 - Windows 2003 Server 64-bit Standard (for 64-Bit Media Indexers)
 - Windows 2008 Server (for AS3000, you need a USB Flash drive)

The Avid System Monitor installer contains a PDF file of this manual in the opennms_config\doc folder.

Software Installation Checklist

The following tables list the Avid System Monitor-related software installation and configuration steps. In general, its best to first install software wherever its needed and configure the servers for SNMP. Then you can move on to configuring the nodes from the OpenNMS interface.

For additional information and for an additional table that shows what to install on each system, see [“Methods for Discovering Systems to be Monitored” on page 110](#)

Software Installation and Configuration on the OpenNMS Server and Individual Nodes

The following table outlines the installation steps as well as configurations that must be performed on the individual nodes.

System	Software Installed/Configured for Monitoring
Network Interface connections ☐	Before you begin configuring the OpenNMS server or configuring a node, check the following: • Disable any unused NICS and make sure that the active NICs are at the top of the binding order. • Make sure that DNS forward and reverse lookup is configured correctly for the system. On a system running the Avid Service Framework, you can check this using the System Check feature in the Workgroup Properties tool.
Avid System Monitor server ☐	Create a local Administrator account on the Avid System Monitor server with a complex password and use the password for the PostgreSQL and OpenNMS installations. See “Preparing the OpenNMS Server” on page 43.

1 Overview and System Requirements

System	Software Installed/Configured for Monitoring
Interplay Engine, Interplay Archive Engine, Interplay Stream Server	☐ Check to see if the Windows SNMP service is running on the Avid System Monitor server. If the service is running, disable it. See “Preparing the OpenNMS Server” on page 43.
	☐ Install Java JDK. See “Installing the Basic OpenNMS Server Software” on page 45.
	☐ Install PostgreSQL (use the above password).
	☐ Install and configure OpenNMS software (use the above password).
	☐ (Option) Install and configure the Avid Service Framework. See “Configuring Time Sync on the Monitoring Server” on page 52.
	☐ Configure Windows SNMP agent. See “Configuring the Windows SNMP Agent” on page 55. For Stream Server, see “Configuring an Interplay Stream Server” on page 67.
	☐ Install and configure Interplay SNMP agent. See “Configuring the Interplay Engine” on page 63.
Avid ISIS System Director	☐ Create an SNMP user on the Interplay database (Interplay engine only). See “Adding an SNMP User to the Interplay Database” on page 65.
	☐ On both ISIS 7000 and ISIS 5000 systems, configure Windows SNMP agent. See “Configuring the Windows SNMP Agent” on page 55.
	☐ On ISIS 5000 systems, run the Enable SNMP Trap Events command. “Configuring the ISIS System Director” on page 68.
Interplay Media Indexer, Interplay Capture, AirSpeed Multi Stream v1.8.1 or higher, General Purpose servers with Lookup service installed	☐ On ISIS 7000 v2.x systems, install the ISIS SNMP agent and run the Enable SNMP Trap Events command. “Configuring the ISIS System Director” on page 68.
	☐ Configure Windows SNMP agent. See “Configuring the Windows SNMP Agent” on page 55.  <i>Before install, check for older Avid SNMP Gateway service and remove it or disable it if present.</i>
	For Media Indexers, see “Configuring a Media Indexer” on page 70.
	☐ Install Avid Monitoring Gateway Service. “Installing the Avid Monitoring Gateway Service” on page 73.

System	Software Installed/Configured for Monitoring	
	☐	For Media Indexers, check the Media Indexer version for the OpenNMS configuration files and make adjustments if necessary. See “Selecting the Software Version of the Media Indexer” on page 70.
Network Switches	☐	Telnet to switch and configure the following: • IP Address of the Avid System Monitor server • Community string for SNMP • Identify the primary interface for sending traps • Specify which switch interfaces should and should not send traps For details, see “Generating SNMP Traps from a Network Switch” on page 74.
Interplay Media Services server and providers, Interplay Transfer, CaptureManager, Interplay Low Res Encoder, iNEWS server	☐	No monitoring software or SNMP configuration required.
Other Intel servers that you want to monitor	☐	No monitoring software or SNMP configuration required.
Avid editing applications	☐	No monitoring software or SNMP configuration required

Configuration From Within the OpenNMS Interface

The following table outlines the steps for configuring the nodes after you’ve performed the software installation.

System	Configuring the Nodes	
Interplay Media Indexer, Interplay Capture, AirSpeed Multi Stream v1.8.1 or higher, network switches, General Purpose servers with Lookup service installed	☐	Use Add Interface command to add the nodes to OpenNMS. See “Using the Add Interface Command to Add Nodes” on page 112.
Network switches	☐	Use Add Interface command to add the nodes to OpenNMS. See “Using Add Interface to Add a Network Switch to OpenNMS” on page 79.

1 Overview and System Requirements

System		Configuring the Nodes
Interplay Engine, Interplay Archive Engine, Interplay Stream Server	☐	Use Provisioning group templates to add the nodes to OpenNMS. See “Configuring a Standalone Interplay Engine” on page 84 and “Configuring Cluster Systems” on page 88 .
Avid ISIS 7000 System Director	☐	Use Provisioning group templates to add the nodes to OpenNMS. See “Using Provisioning Groups to Configure an ISIS 7000 System Director” on page 101
Avid ISIS 5000 System Director	☐	Use the Add Interface command to add the node to OpenNMS. See “Using the Add Interface Command to Add Nodes” on page 112 .
Interplay Media Services server and providers, Interplay Transfer, CaptureManager, Interplay Low Res Encoder, iNEWS server	☐	Add to NodeUpDown Provisioning group. This provides a real-time inventory of the system status. See “Defining Nodes with Basic Up/Down Status” on page 103 .
Other Intel servers that you want to monitor	☐	Add to NodeUpDown Provisioning group. See “Defining Nodes with Basic Up/Down Status” on page 103 .
Configure the OpenNMS Dashboard	☐	After the nodes are added to OpenNMS, its time to create a view of the system. See “Configuring the Dashboard” on page 113 .
Configure Email Notification and Maps	☐	These are optional steps. See “Working With Notifications and Maps” on page 121 .

Configuration Files

The following tables lists the configuration files that are added or modified for the Avid monitoring solution. These files are on the Monitoring Software installer and are copied onto the Avid System Monitor system as part of the installation and configuration procedure.

Function	Configuration Files
Monitoring	/etc/capsd-configuration.xml /etc/collectd-configuration.xml /etc/datacollection-config.xml /etc/eventconf.xml /etc/http-datacollection-config.xml /etc/poller-configuration.xml /etc/snmp-graph.properties /etc/threshd-configuration.xml etc/thresholds.xml

Function	Configuration Files
Notifications	/etc/notifd-configuration.xml /etc/destinationPaths.xml /etc/notificationCommands.xml /etc/notifications.xml
Global Avid System Monitor System settings	/etc/snmp-config.xml /etc/discovery-configuration.xml /etc/imports-***.xml /etc/opennms.conf
Dashboard Related	/etc/service-configuration.xml /etc/linkd-configuration.xml /etc/surveillance-views.xml /etc/map.enable /etc/categories.xml /etc/viewsdisplay.xml /etc/map.properties
Avid event files	/Etc/events/AvidISIS.events.xml Etc/events/avidinterplaymediaindexter.events.xml Etc/events/avidlookupservice.events.xml Etc/events/avidworkflowengine.events.xml Etc/events/avidvtrdeviceservice.events.xml Etc/events/avidsharedstorageservice.events.xml Etc/events/avidrouteengineservice.events.xml Etc/events/avidairspeeddeviceservice.events.xml Etc/events/avidcaptureservice.events.xml Etc/events/avidinterplaymediaservices.events.xml Etc/events/avidlicensingsservice.events.xml Etc/events/avidworkstationservice.events.xml Etc/events/avidtimesynchronizationsservice.events.xml Etc/events/avidsystemconfigurationsservice.events.xml Etc/events/avidservicestartersservice.events.xml Etc/events/avidmachinemonitorservice.events.xml Etc/events/avidlocaldiscoveryservice.events.xml Etc/events/avidmonitoringgatewaysservice.events.xml Etc/events/AvidInterplayEngine.events.xml Etc/events/transfermanager.events.xml Etc/events/AvidStreamingServer.events.xml Etc/events/AvidIsis21.events.xml Etc/events/avidisismonitoringservice.events.xml Etc/events/avidmonitoringgateway.events.xml Etc/events/force10.events.xml Etc/events/Translator.default.events.xml

Function	Configuration Files
Library files	/Lib/dnsjava2.0.2.jar /Lib/avidextensions.jar (enables DNS and Timesync verifications)

Backing Up the Avid System Monitor Files

Avid recommends that you periodically backup the PostgreSQL database and the OpenNMS configuration files. The OpenNMS configuration files contain the Avid specific configuration files as well as configuration files that are modified as you name nodes, create events or notifications.

For information on backing up and restoring files, see [“To Perform a Complete Backup of Avid System Monitor” on page 192](#) and [“Backing Up and Restoring the PostgreSQL Database” on page 192](#).

2 Getting Started with OpenNMS

This chapter describes some of the basic operations that you will perform with the OpenNMS interface.

- [New for Avid System Monitor v1.2.1](#)
- [New for OpenNMS v1.8.10](#)
- [The OpenNMS Main Page](#)
- [The Dashboard and Surveillance View](#)
- [Resource Graphs and Reports](#)
- [The Map Page](#)
- [The Search Page](#)

New for Avid System Monitor v1.2.1

There are two sets of new features for Avid System Monitor v1.2.1:

- New features for Avid System Monitor - these are features added by the Avid System Monitor team.
- New features for OpenNMS v1.8.10 - these are new features specific to OpenNMS v1.8.10.

New Features for Avid System Monitor

The Avid System Monitor team has added the following features for v1.2.1:

- Support for OpenNMS v1.8.10
- Support for Avid AirSpeed Multi Stream v1.8.1 and higher
- Support for a procedure to back up and restore the PostgreSQL database and the OpenNMS configuration files. [“To Perform a Complete Backup of Avid System Monitor” on page 192](#)
- Support for an upgrade utility that allows you to upgrade a v1.1.1 system to v1.2.1. This will maintain the PostgreSQL database history, the node list, and many of the customizations you made on your v1.1.1 system. See [“Running the Avid System Monitor Upgrade Utility” on page 186](#).

New for OpenNMS v1.8.10

Avid System Monitor v1.2.1 supports OpenNMS v1.8.10. The following areas are new or changed for this release:

- Provisioning Groups
- The Resource Graphs Interface. See [“Working with Resource Graphs” on page 163](#).

The following section describes the changes to provisioning groups. For a complete description, see [“Working with Provisioning Groups” on page 83](#).

Changes to Provisioning Groups

The process for creating provisioning groups is different starting at v1.8.0. Provisioning groups allows you to specify which services are going to be monitored on a node. This simplifies the monitoring process and allows you to monitor only the recommended services.

New Location for Provisioning Group Templates

The provisioning group templates are now located in the following directory:

OpenNMS\etc\imports

In addition, the template files no longer have the text “imports-” appended to the beginning of the file. For information on working with the provisioning group templates, see [“Working with Provisioning Groups” on page 83](#).

Changes to the Provisioning Groups User Interface

The user interface for creating provisioning groups has changed. For details on the changes, see the OpenNMS Provisioning white paper on the OpenNMS web site:

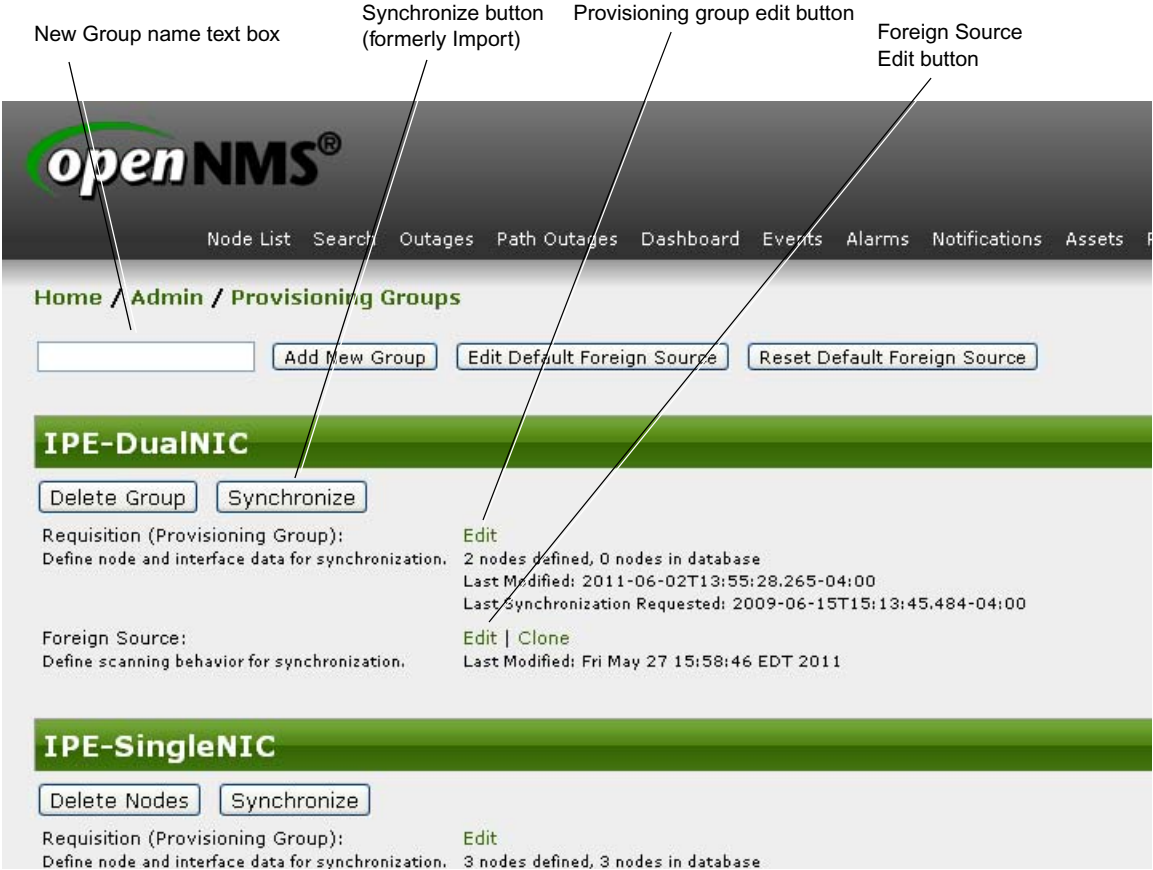
http://www.opennms.org/wiki/White_Papers

The following procedure describes how to work with the new interface.

To edit Provisioning Groups:

1. Click the Admin link in OpenNMS.
2. Under the Nodes section, click Manage Provisioning Groups.

The Provisioning Groups window opens. The following illustration shows the Avid System Monitor provisioning group page and the new user interface elements.



The following table describes the new or changed user interface elements.

Option	Description
New Group name text box	Enter a name when creating a new provisioning group. Then click Add New Group.
Synchronize button	Imports the provisioning group changes to OpenNMS. Formerly called the Import button.
Provisioning group edit button	Allows you to edit the provisioning group.
Foreign Source edit button.	Contains “detectors” that automatically monitor specific services. When you create a new provisioning group, click the Edit button and delete all of the detectors for that group. They are not required and may cause unnecessary services to be monitored.

2 Getting Started with OpenNMS

For information on working with provisioning group templates, see [“Working with Provisioning Groups” on page 83](#).

Changes to ISIS Client Service Name for ISIS v2.3 and Later

If you are running ISIS v2.3 or later in your Interplay environment, you must make a change to the default provisioning group. See [“Interplay Engines and ISIS v2.3 and v2.4” on page 94](#).

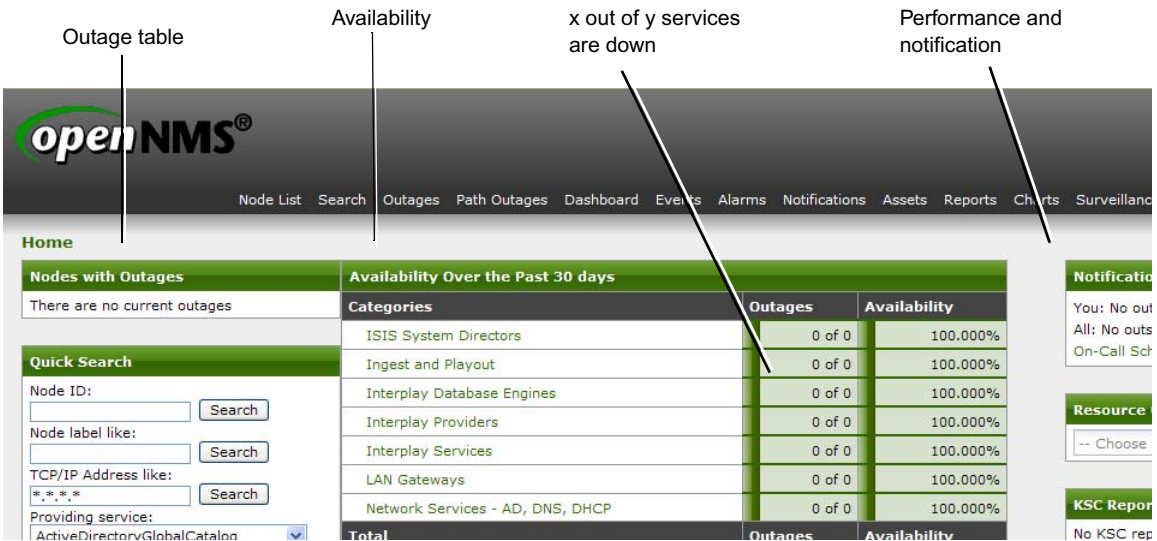
Terminology

The following are the main terms associated with OpenNMS monitoring.

- **Node** – One of the systems that is being monitored. For example, an Interplay server, an ISIS System Director, or a network switch.
- **Service Polling** - determining service availability and latency, and reporting on the results.
- **Data Collection** - collecting, storing and reporting on data collected from nodes via ICMP, SNMP and HTTP protocols.
- **Thresholding** - evaluating polled latency data or collected performance data against configurable thresholds, creating events when these are exceeded or rearmed.
- **Outage** – a temporary suspension of operation signified by the inability to communicate with a managed service. The node could be running but the service is down or unavailable.
- **Event** - any defined event, including SNMP traps. For example, an event is generated if a cluster services is down, or the Interplay agent detects a large number of deletes.
- **Alarm** - any significant event. Alarms are defined and based on one or more occurrences of events. Each alarm displays the number of related events.
- **Notification** – a notice sent out when specific events occur. Usually consists of making users or groups of users aware of events via email.

The OpenNMS Main Page

When you first log into the OpenNMS application, the system displays the Main page. From this centralized view, you can obtain a quick overview of the current health of the monitored nodes. The following illustration shows an example.



- The upper right hand corner contains information about the time and date on the OpenNMS server, as well as the currently logged in user, and whether or not notifications are currently turned on.



For information on how to turn notifications on, see “Working with Email Notifications” on page 121.

- **Outage Table:** To the left of the screen is the outage table, labeled "Nodes with Outages." This is a list of nodes that currently have service outages. Clicking on a node in this list presents more specific information about the node, it's services, and current, as well as historic, outages. From this page, information can be found regarding times that any outages occurred as well as when service was restored. For additional information, see “Examine the Home Page and Dashboard” on page 157. You can also perform a quick search for nodes or services from this part of the interface.
- **Availability:** In the center of the display are categories of services. For each category, there is listed the number of current service outages as well as availability for the last 30 days. These categories are directly related to the categories on the OpenNMS dashboard. For example, the “Interplay Engine Databases” and “Interplay Services” categories on the dashboard are included in the Interplay category on the Main page.

Outages are based on the services running on a node. For example, in the Interplay row in the above illustration there are 8 of 153 outages. This lab does not have 153 nodes in the Interplay category. There are less than a dozen Interplay servers. But the total number of services on those nodes adds up to 153. This section provides a calculation of the availability of these services from a up-time perspective over the past 30 days.

- Performance and Notification: On the right side of the display there are links to notifications and a portal to Resource graphs and KSC reports. This section is used to create graphs from data collected by OpenNMS. For additional information, see [“Resource Graphs and Reports” on page 39](#).

The Node List

Click Node List on the left edge of the OpenNMS display. The list displays all of the nodes that have been added. Some nodes may have names while others have their Domain names.

Node List Search Outages Path Outages Dashboard Events	
Home / Search / Node List	
Nodes	
a51-wg1-eng1.global.avidww.com	A51WG1ABCluster.glc
a51-wg1-eng2.global.avidww.com	ISIS SD a51-wg1-sd1
A51-WG1-GPS1.global.avidww.com	Media Indexer A51-W
6 Nodes Show interfaces	

There are two types of names in the above illustration as follows:

- Fully qualified domain names. Domain names are assigned automatically as part of the discovery process.
- The names that start with “ISIS SD” and “Media Indexer” have been named by the Administrator. For information on naming nodes, see [“Naming the Discovered Nodes” on page 119](#).

You can click on any of the nodes in the list to display the node’s information page. For example, the following illustration shows the information page for a Media Indexer. The list of discovered services are displayed on the left and the recent events and notifications are displayed on the right.

Home / Search / Node
Node: docmi.global.avidww.com
[View Events](#) [View Alarms](#) [Asset Info](#) [Resource Graphs](#) [Rescan](#) [Admin](#) [Update SNMP](#)

General (Status: Active)		
View Node Link Detailed Info		
Availability		
Availability (last 24 hours)	100.000%	
10.106.50.12	Overall	100.000%
	AvidISISClient	100.000%
	AvidInterplayMediaIndexer	100.000%
	AvidLookupService	100.000%
	AvidMachineMonitorService	100.000%
	AvidMonitoringGatewayService	100.000%
	AvidServiceStarterService	100.000%
	AvidSystemConfigurationService	100.000%
	AvidTimeSynchronizationService	100.000%
	ICMP	100.000%
SNMP	100.000%	

Notification	
You: Outstanding:	(Check)
You: Acknowledged:	(Check)
Recent Events	
☐ 5591	8/19/10 18:18:39
☐ 5589	8/19/10 18:18:39
☐ 5588	8/19/10 18:18:39
☐ 5587	8/19/10 18:18:39
☐ 5586	8/19/10 18:18:39
Acknowledge Reset More	
Recent Outages	
There have been no outages on t	

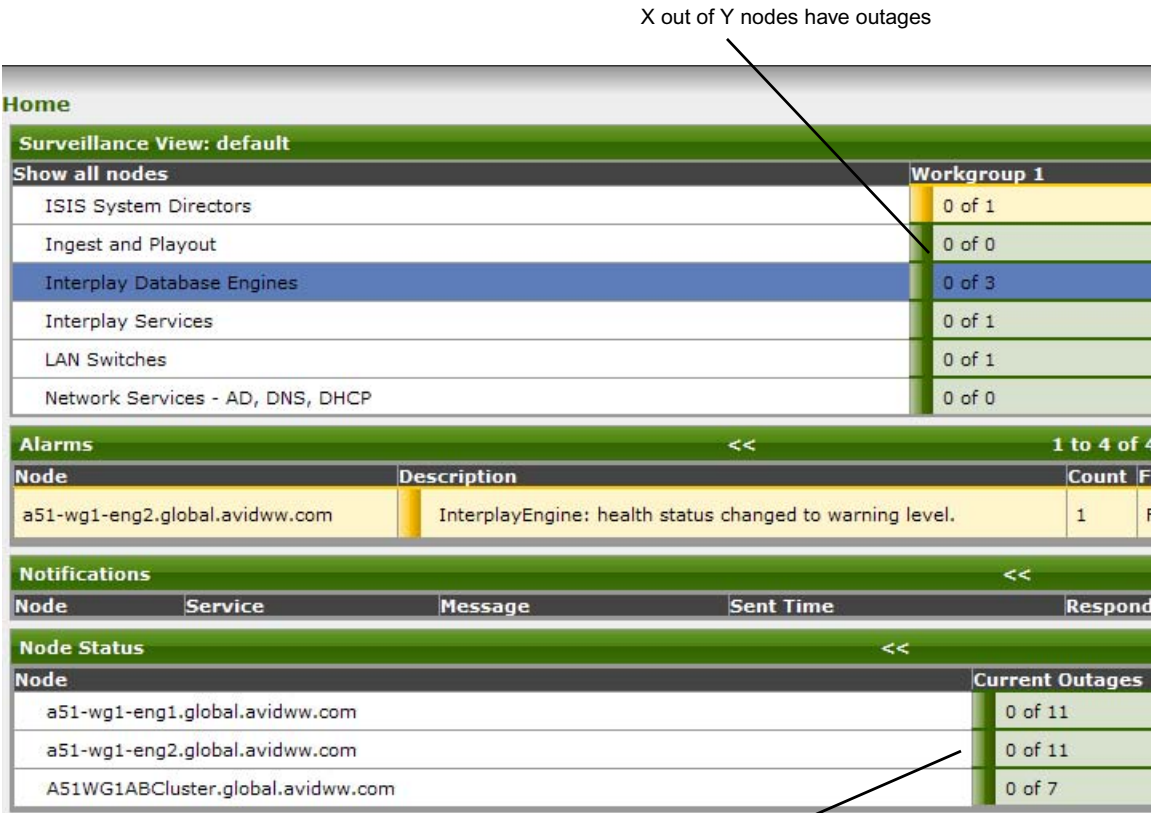
You can see from the above illustration that this node is running the AvidInterplayMediaIndexer service and that it is also an ISIS client (it is also running the AvidISISClient service). The IP address on the left is the interface that is running the services. Interfaces correspond to network interface cards (nics). Some nodes have more than one nic and therefore have multiple interfaces. For example, a Media Indexer often has two interfaces. Media Indexer is one of the nodes that uses Add Interface or “automatic discovery” to determine the services and interfaces running on the node. You specify one IP address and the system automatically determines the other interface. Other nodes such as Interplay Engine or ISIS System Director use an OpenNMS feature known as provisioning groups to register only specific services and interfaces with OpenNMS. For information on how OpenNMS discovers services, see [“An Example Monitoring Workflow for Automatic Discovery”](#) on page 19.

The Dashboard and Surveillance View

The dashboard provides a snapshot of the health of machines in the various groups. The Dashboard is one of the user interface items that must be configured on site. For information, see “Configuring Discovery and the Dashboard” on page 109.

 *The Dashboard and Surveillance views display an error until you configure the dashboard.*

The following illustration shows an example of the dashboard.



X out of Y services on this node have outages

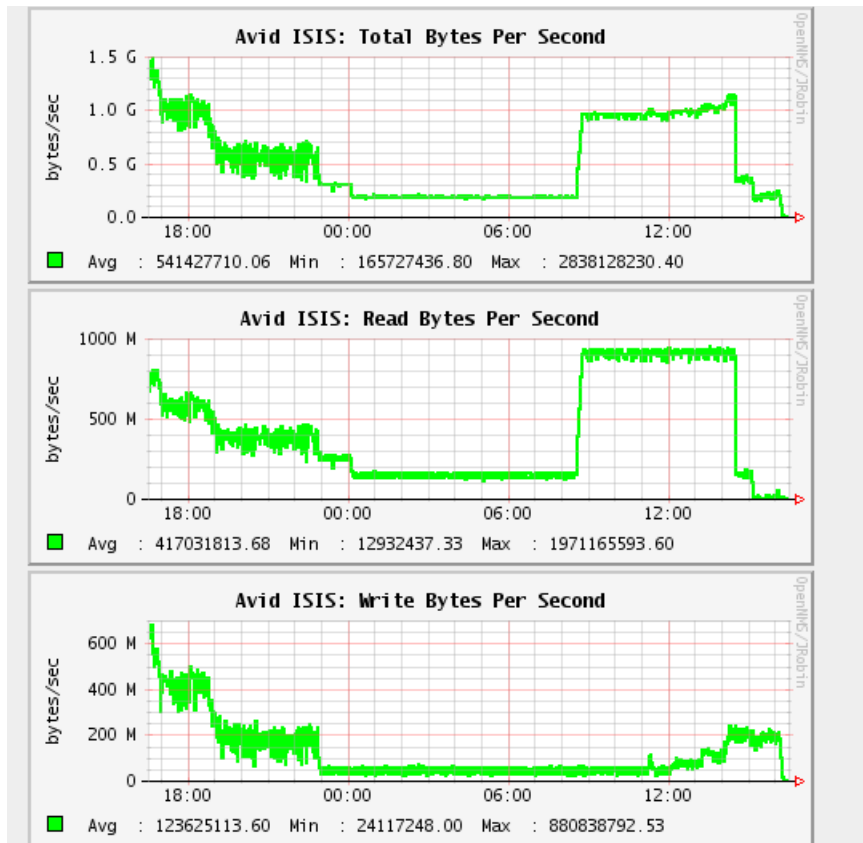
In the above illustration there are three nodes in the Interplay Database Engines category. They are listed at the bottom. Note the difference between node outages and service outages.

 *To find out information on a particular node in the Node Status list, copy part of the name, open the Search page, and paste the name into the “Name containing” field.*

The Surveillance View shows just the categories section of the Dashboard without the alarms and notification sections. This can be useful for a quick glance at the system for outages. Choose the Surveillance link from the top of the OpenNMS interface.

Resource Graphs and Reports

Many of the items that Avid System Monitor monitors can be displayed in graphs that show how the values change over time. You can view all of the graphs for a particular system or you can also create custom reports that you can use to display the data from a number of different systems on the same page. The following illustration shows the bandwidth resource graphs for an ISIS System Director.



The following illustration shows a custom report that displays the Read and Write bandwidth for two different System Directors.

2 Getting Started with OpenNMS

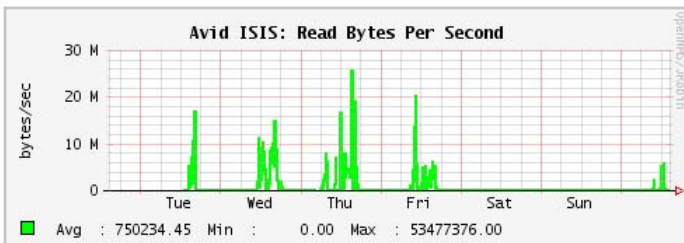
Home / Reports / KSC Reports / Custom View

Custom View: ISIS Read/Write bandwidth

A51-WG1-SD1

From: Mon Aug 22 14:27:21
EDT 2011
To: Mon Aug 29 14:27:21 EDT
2011

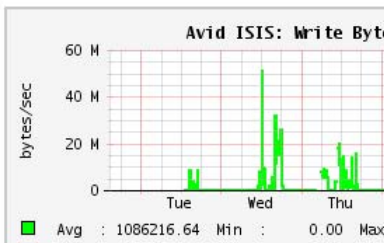
Node: [a51-wg1-sd1.global.avidww.com](#)
SNMP Node Data: Node-level Performance
Data [Detail](#)



A51-WG1-SD1

From: Mon Aug 22 14:27:21
EDT 2011
To: Mon Aug 29 14:27:21 EDT
2011

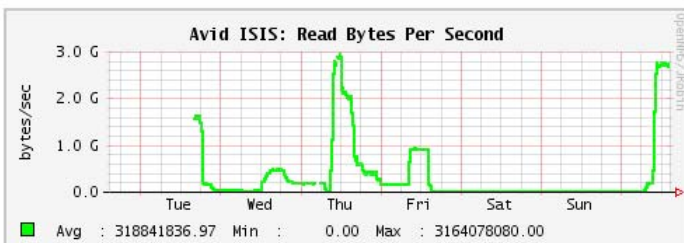
Node: [a51-](#)
SNMP Node
Data [Detail](#)



b3index02

From: Mon Aug 22 14:27:21
EDT 2011
To: Mon Aug 29 14:27:21
EDT 2011

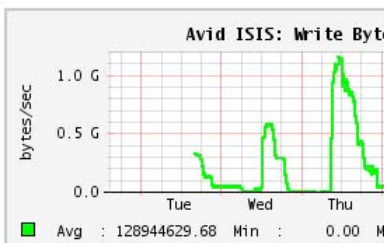
Node: [b3index02.global.avidww.com](#)
SNMP Node Data: Node-level Performance
Data [Detail](#)



b3index02

From: Mon Aug 22 14:27:21
EDT 2011
To: Mon Aug 29 14:27:21
EDT 2011

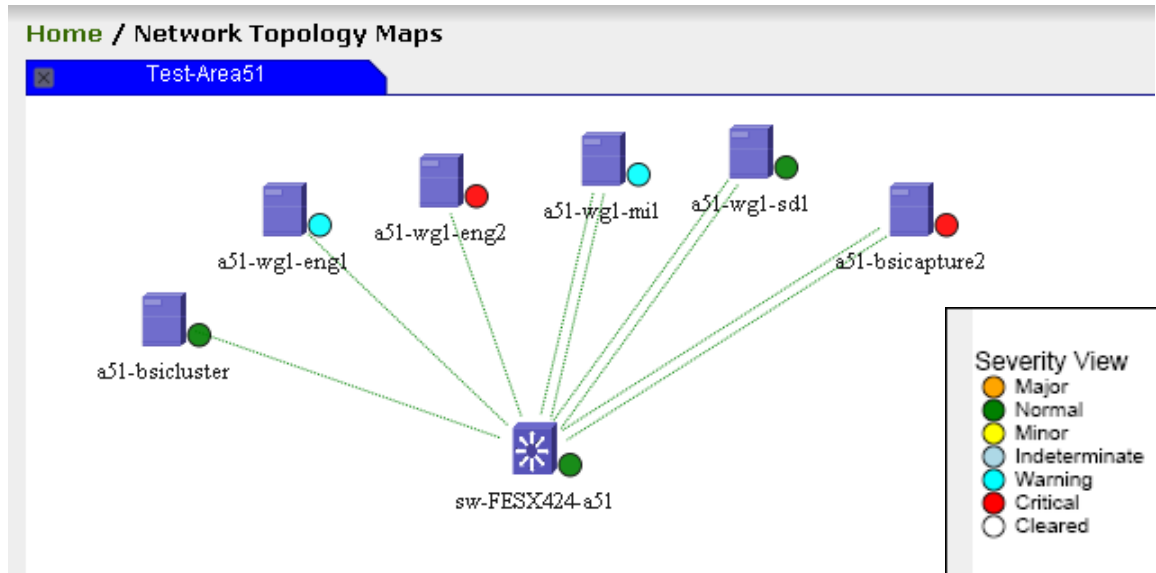
Node: [b3ind](#)
SNMP Node
Data [Detail](#)



For additional information, see “Working with Resource Graphs” on page 163 and “Creating Reports” on page 167.

The Map Page

You can configure maps to provide a visual display of different aspects of your environment. For example, the following illustration shows a map of several servers in an Interplay environment.



In the above illustration, there are critical events associated with the nodes with red circles. You can double click on the node in the map and go directly to the node's information page to find out more information on the problem. For additional information, see [“Working with Maps” on page 138](#).

The Search Page

Click on the Search link to open the search page. From here you can search for nodes using various criteria. Once a search is initiated you receive a list of nodes and their interfaces that match the search criteria. Each of these will be a link to the main node, or interface pages. These pages contain a very complete set of information about each device. The Search page describes the criteria options you can use. The following illustration shows an example of searching for a specific service such as the Lookup Services.

Searching for nodes running the Lookup service.

Home / Search

Search for Nodes

Name containing:

TCP/IP Address like:

IfAlias containing:

Providing service:

Mac Address like:

[All nodes](#)

[All nodes and their interfaces](#)

You can generate lists of nodes that match any of a number of criteria including IP addresses, services, and machine names. Ranges of addresses can be entered for example, to provide a list of nodes that have IP addresses in that range. There are examples in the Search Options section of the page, as well as some syntax rules to help refine searches.

3 Installing Software on the Avid System Monitor Server

This chapter describes how to install and configure software on the Avid System Monitor server.

- [Upgrading from Avid System Monitor v1.1.1](#)
- [Preparing the OpenNMS Server](#)
- [Installing the Basic OpenNMS Server Software](#)
- [Restarting or Stopping OpenNMS](#)
- [Uninstalling Avid System Monitor](#)
- [Configuring Time Sync on the Monitoring Server](#)

Upgrading from Avid System Monitor v1.1.1

Avid System Monitor v1.2.1 supports an upgrade tool that allows you to upgrade from a v1.1.1 installation to v1.2.1. For details, see [“Running the Avid System Monitor Upgrade Utility” on page 186](#).

Preparing the OpenNMS Server

This section describes how to prepare the OpenNMS server.

To initialize the system:

- ▶ If the system is a repurposed Intel SR2400 or SR2500, use the appropriate Interplay Engine Recovery DVD to initialize the system before installing the OpenNMS software. See [“What to Bring to an Installation” on page 24](#).

The Interplay Engine Recovery DVD contains the Windows Server 2003 software and can be used to initialize the Avid System Monitor server.

- ▶ If the system is an AS3000, use the same image as an Interplay Engine: Windows Server 2008 R2 64-bit and install the 32-bit version of OpenNMS. You must also disable the ATTO ConfigTool Service as shown in the following illustration.

3 Installing Software on the Avid System Monitor Server

ce

Name	Description	Status	Startup Type	Log On As
Application Experience	Processes ...		Manual	Local System
Application Host Helper Service	Provides a...	Started	Automatic	Local System
Application Identity	Determines...		Manual	Local Service
Application Information	Facilitates ...		Manual	Local System
Application Layer Gateway Service	Provides s...		Manual	Local Service
Application Management	Processes i...		Manual	Local System
ASP.NET State Service	Provides s...		Manual	Network S...
ATTO ConfigTool Service	Manages a...		Automatic	Local System
Background Intelligent Transfer Service	Transfers f...	Started	Manual	Local System
Base Filtering Engine				
BITS Compact Server				
Certificate Propagation				
CNG Key Isolation				
COM+ Event System				
COM+ System Application				
Computer Browser				
Credential Manager				
Cryptographic Services				
DCOM Server Process Launcher				
Desktop Window Manager Session Man...				
DHCP Client				
Diagnostic Policy Service				
Diagnostic Service Host				
Diagnostic System Host				
Disk Defragmenter				
Distributed Link Tracking Client				

TO storage
with the ATTO

Manufacturer:	Avid
Processor:	Intel(R) Xeo
Installed memory (RAM):	12.0 GB
System type:	64-bit Oper
Pen and Touch:	No Pen or To

Avid support

ATTO ConfigTool Service Properties (Local Computer)

General

Log On

Recovery

Dependencies

Service name:

atmtgtd

Display name:

ATTO ConfigTool Service

Description:

Manages and monitors ATTO storage controllers in coordination with the ATTO Configuration Tool.

Path to executable:

C:\PROGRA~2\ATTO\CO~1\atmtgtd.exe

Startup type:

Disabled

[Help me configure service startup options.](#)

Service status:

Stopped

Start

Stop

Pause

Resume

You can specify the start parameters that apply when you start the service from here.

Start parameters:

OK

Cancel

Apply

To create a local Admin user on the Avid System Monitor system:

1. Create a local Admin account on the system that will run the OpenNMS software. You will use this account and password to install the PostgreSQL and OpenNMS software. For example, set up an admin account named AdminNMS.

Make sure the login password meets the site security restrictions. Use a complex password that contains at least one occurrence of the following:

- Capital letter
- Lower case letter
- Special character

- Numeral

For example, the following password meets the complexity requirements: Av1dnm\$. The PostgreSQL installation software creates a PostgreSQL user that uses this password. The OpenNMS software uses the password and user to access the PostgreSQL database. The only users that need access to this account are the people responsible for installing and updating the Avid System Monitor software. It is a good idea to decide on a consistent username and password across your organization.

To disable SNMP on the Avid System Monitor system:

1. Log onto the system with the local Avid System Monitor Admin account.
2. Right-click the My Computer icon on the desktop and select Manage. Navigate to the Services section and determine whether the following services are running:
 - SNMP Service
 - SNMP Trap Service
3. If the SNMP services are running, stop and disable them. The services should not be running on the Avid System Monitor system.

Installing the Basic OpenNMS Server Software

This section describes how to install the following software:

- Java JDK - you need to install a full JDK rather than just a Java run time environment
- PostgreSQL database software
- OpenNMS standalone installer for Windows
- Avid-specific configuration files for OpenNMS
- Avid Service Framework



The Avid Monitoring System service is automatically installed by the script that installs the Avid-specific configuration files. After the install you must check whether the service is running and start it if necessary.

All of the installers are available on the Avid System Monitor Software installer.

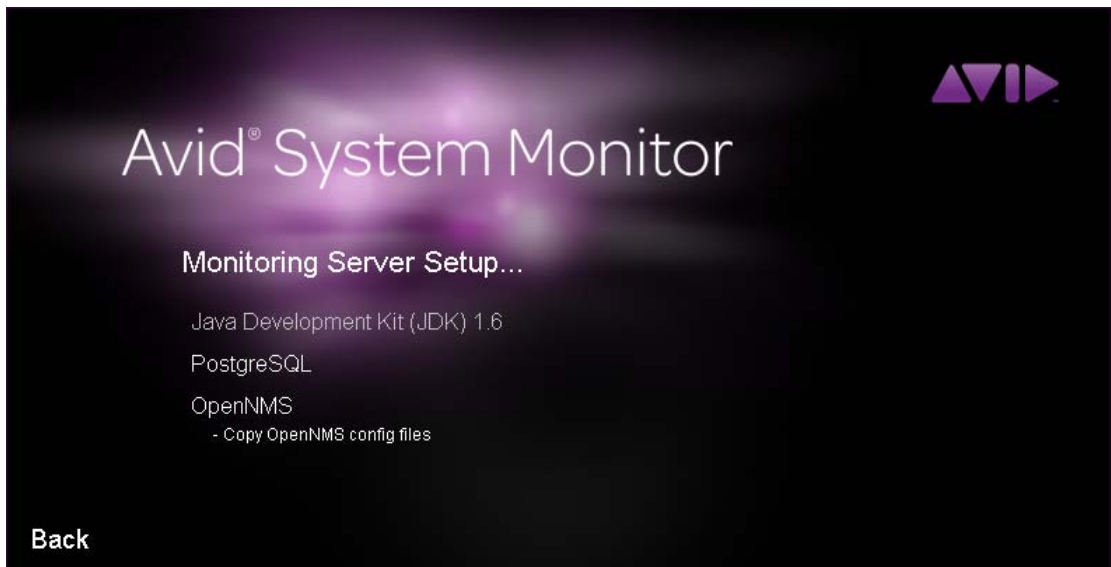
3 Installing Software on the Avid System Monitor Server

To start the Avid System Monitor installer:

1. Launch the Avid System Monitor installer. The Main installer page opens.



2. Click Monitoring Server Setup. The Monitoring Server Setup window opens.



To install Java, PostgreSQL, and OpenNMS:

1. Install the Java JDK software and note the installed location. You will need the location for the OpenNMS installation. For example:

C:\Program Files\Java\jdk1.6.0_13

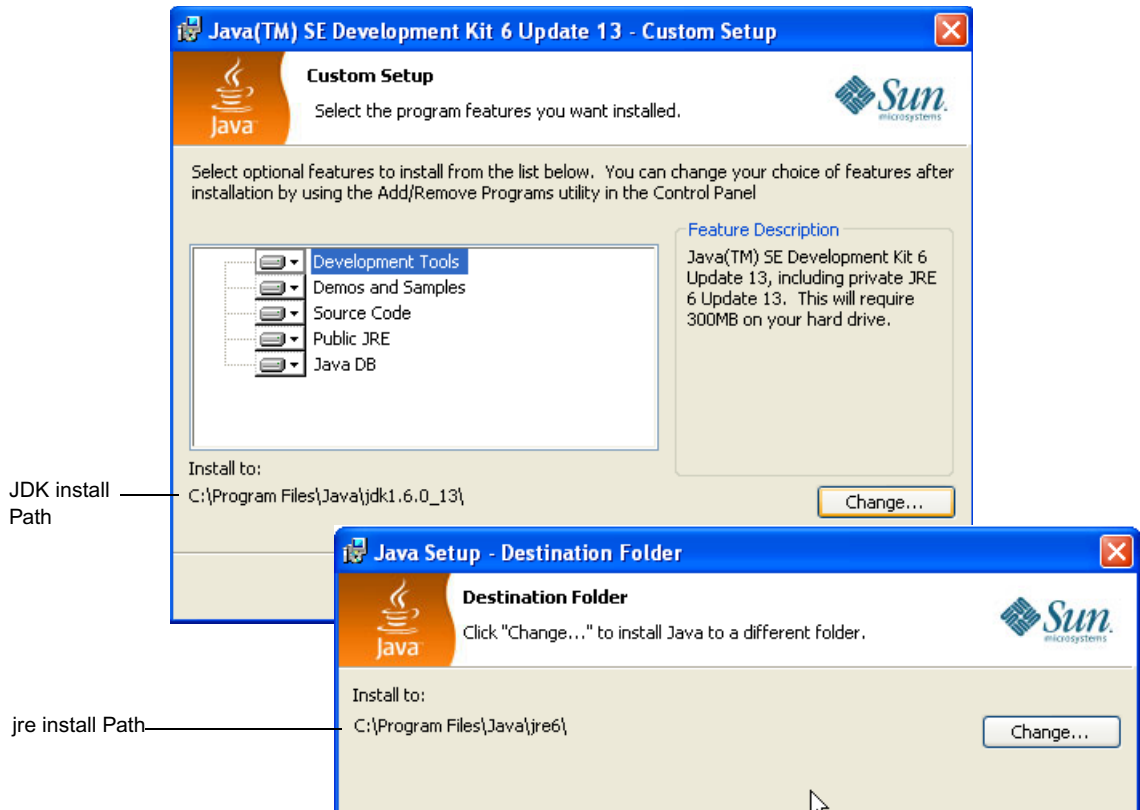


Install all three software applications (Java, PostgreSQL, and OpenNMS) on the same drive. For example, install them all on the C:\ drive or install them all on the D:\ drive.



On a 64-bit system, install the 32-bit versions of Java, OpenNMS, and PostgreSQL. the 64-bit version of OpenNMS is not supported for Avid System Monitor v1.2.1.

The installer prompts for two installation paths: one for the jre software and one for the jdk. Install both on the same drive. The following illustrations show the two dialog boxes that require a path.



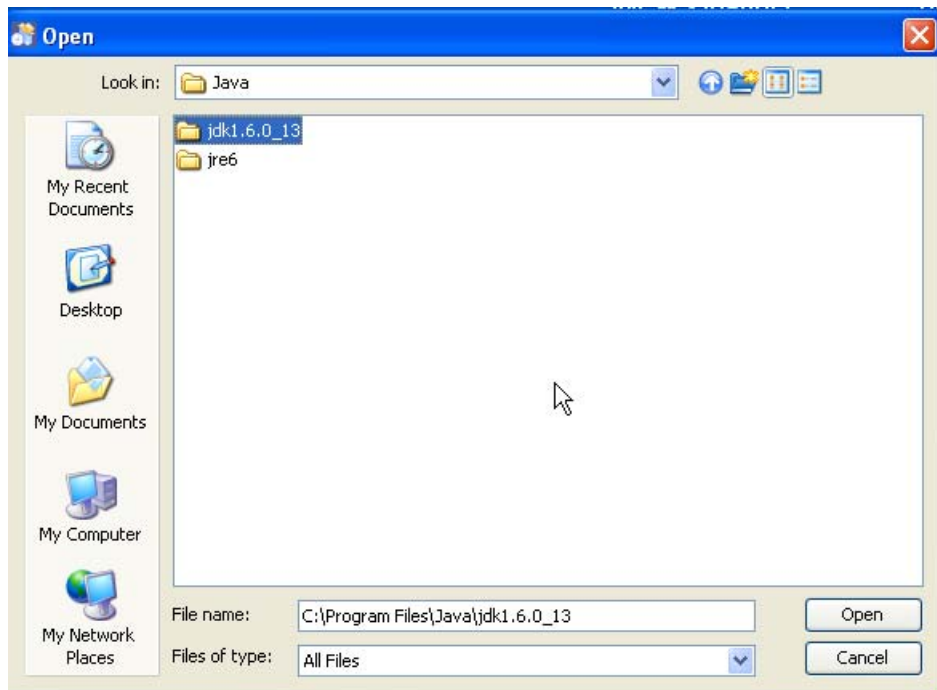
Make sure you point both installation paths to the same drive.

3 Installing Software on the Avid System Monitor Server



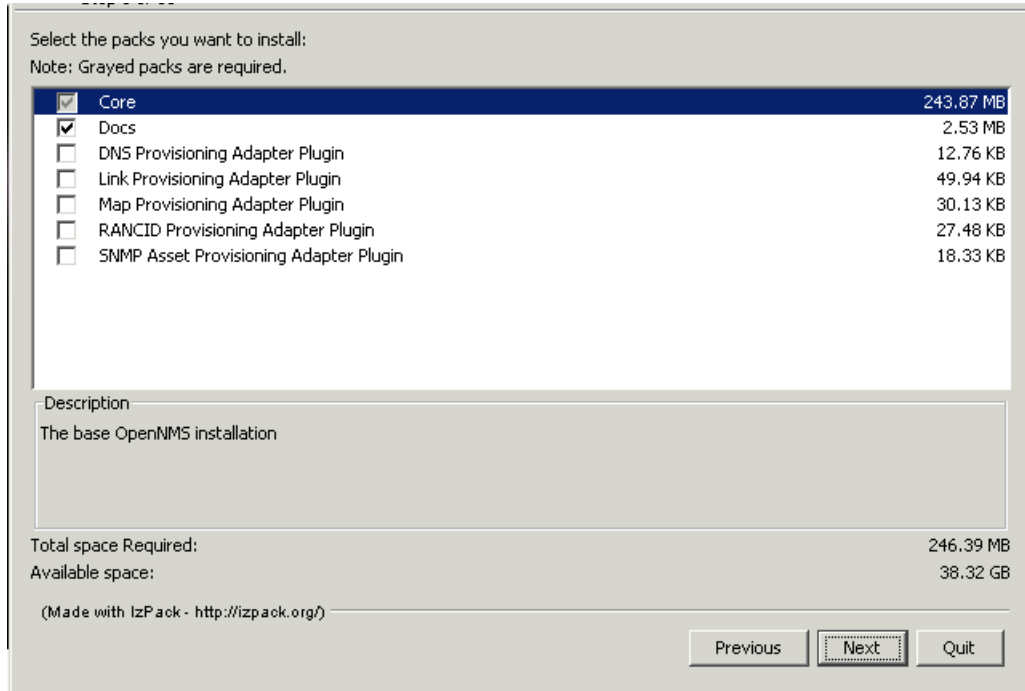
At the end of the Java install the installer launches a web browser to check for updates. You can ignore the request and close the browser.

2. Install the PostgreSQL database software, The software will ask for a password. Supply the local Avid System Monitor Admin login password. If the password does not meet the security requirements the install will fail. See “To create a local Admin user on the Avid System Monitor server” earlier in this section.
3. At the end of the PostgreSQL install, a dialog box asks if you want to use StackBuilder to install additional software, Deselect the checkbox and click Finish. The Stackbuilder software is not required by OpenNMS.
4. Install OpenNMS. Use the default values with the following caveats:
 - a. Supply the password you used for the PostgreSQL install.
 - b. When prompted, navigate to the folder where you installed the Java JDK software and click Open. The following illustration shows the selected path.



- c. The installer prompts you to select from a list of plug-ins. Just select the default Docs option. Do not select any of the plug-ins for this release.

Do not
select
any of
the
plug-ins.



The plug-ins have not been qualified for this release. Do not select any during the installation.

- d. The installation prompts you to add a Discovery Range of IP addresses. Click Next to accept the default range. You will delete the range later during the configuration process.

To copy the Avid configuration files and install the Avid System Monitor Service:

1. Click Copy OpenNMS config files.

The installer performs the following operations:

- a. Creates a backup of the Program Files/OpenNMS/etc directory named etc_back.
- b. Copies the Avid-specific config files into the appropriate locations.
- c. Runs a script that creates the Avid System Monitor service. This is the service you will use to stop and start OpenNMS.



The system does not display a progress bar during the operation. It displays a dialog box once the operation is complete.

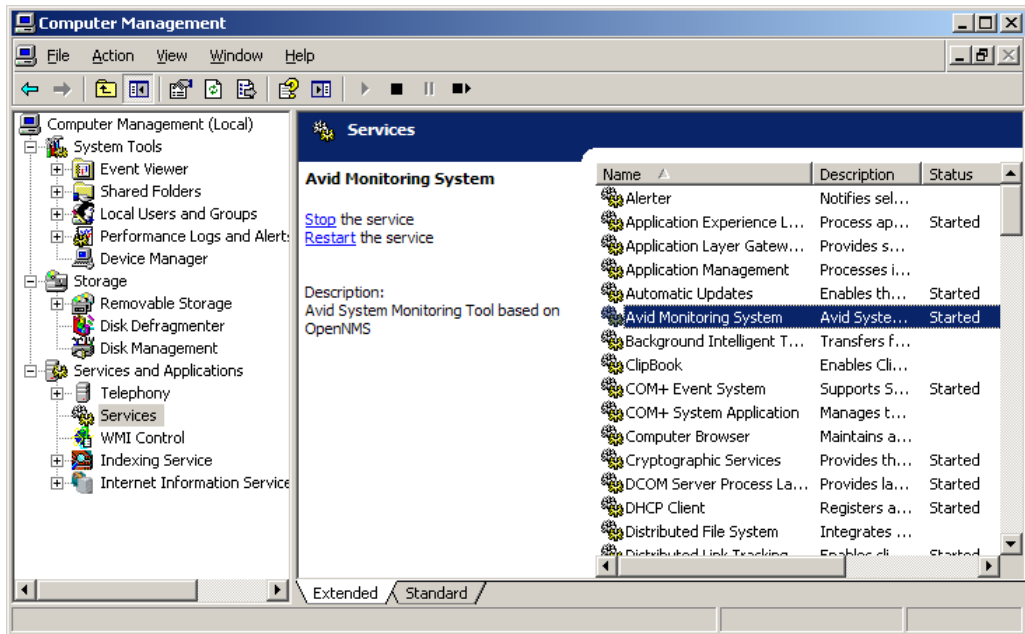
3 Installing Software on the Avid System Monitor Server



If you need to copy the Avid configuration files manually, open the `opennms_config` folder on the installer and copy the folders in that directory to `Program Files\OpenNMS`, overwriting the existing folders.

To ensure that the Avid Monitoring System service is running:

1. Open the Windows Service Manager and locate the Avid Monitoring System service.
2. If necessary, start the Avid Monitoring System service.



To launch the Avid System Monitor (OpenNMS) application:

1. Open a browser window and enter one of the following URL values:
 - `http://localhost:8980/opennms`
 - `http://<Avid System Monitor IP address>:8980/opennms`

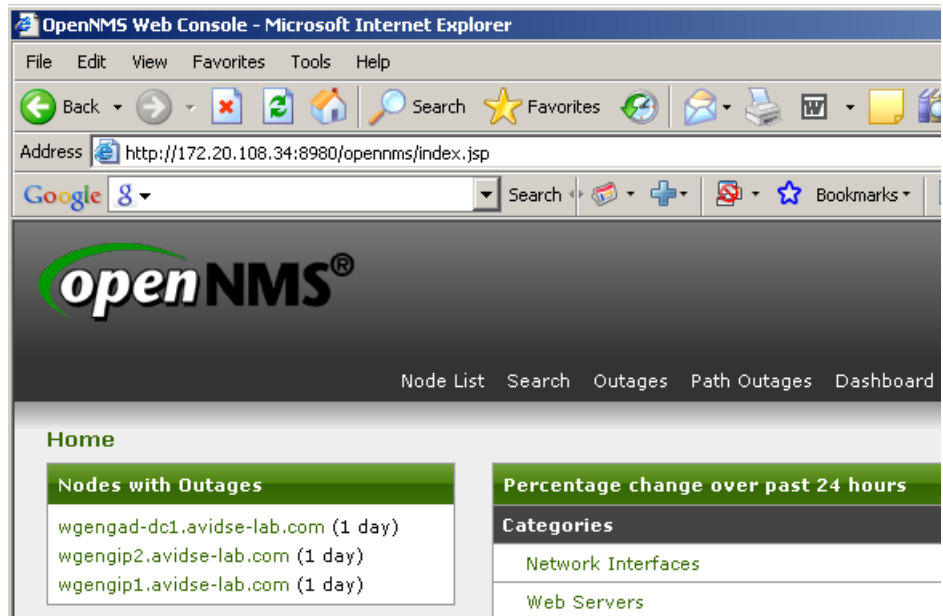
For example, `http://172.20.108.34:8980/opennms`



You can use the IP address to log open the Avid System Monitor interface from any system on your network.

2. Use the following default login credentials:
 - user: admin
 - password: admin

The following illustration shows the home page of the OpenNMS interface.



Restarting or Stopping OpenNMS

Restarting OpenNMS application and restarting the Avid System Monitor application are interchangeable terms.

To start or stop Avid Monitoring System service (start and stop OpenNMS):

1. Open the Windows Service Manager and locate the Avid Monitoring System service.
2. Start, stop or restart the Avid Monitoring System service as necessary.

You will need to reload the OpenNMS web page after the application restarts.

Uninstalling Avid System Monitor

If you need to do a clean install on a server already running the Avid System Monitor, it is best to uninstall OpenNMS, PostgreSQL, and (optionally) the Java JDK.

To uninstall the Java, PostgreSQL, and OpenNMS software:

1. If you have performed configuration tasks such as adding nodes, defining provisioning groups, or setting up email notifications, backup the database as described in [“To Perform a Complete Backup of Avid System Monitor” on page 192.](#)
2. Stop the OpenNMS service. See [“Restarting or Stopping OpenNMS” on page 51.](#)
3. Use the OpenNMS uninstall program in the following directory:

Program Files\OpenNMS\uninstall

4. Use Control Panel Add/Remove Programs to uninstall PostgreSQL. This will require a reboot.
5. Delete the Postgres user in the Computer Management application.
6. (Option) Use the Control Panel to uninstall the Java JDK and the Java jre.
7. Delete the following directories:

Program Files\OpenNMS

Program Files\PostgreSQL

Deleting the directories guarantees a clean install in case you want to reinstall OpenNMS.

For a procedure to backup and restore the database, see [“Backing Up and Restoring the PostgreSQL Database” on page 192.](#)

Configuring Time Sync on the Monitoring Server

It is important that the Avid System Monitor (OpenNMS) server uses the same method of Time Sync as the other systems in your Interplay environment. The Avid System Monitor displays a warning if any of the nodes that you are monitoring are more than 30 seconds out of sync with the time used by the Avid System Monitor.

- If you use NTP or Active Directory to maintain time sync on your network, make sure that the OpenNMS server is synced to the same time source.
- If you use the Avid Service Framework for Time sync, install a client version of the framework on the Avid System monitor. Then configure the Time Sync service to be in Slave mode to match the time of the system you use to maintain time sync on your network

If you need to install the Avid Service Framework, install the same version of the framework that you are running in your Interplay environment.

To install the Avid Service Framework:

1. Locate the Interplay Installer DVD or USB flash drive that matches the Interplay version running at your site.
2. Run the Avid Service Framework installer and select the Client option. Install the following components of the Avid Service Framework.
 - Service Configuration
 - Avid Diagnostics
 - Avid Health Monitor service
 - Avid Machine Monitor service
 - Time Synchronization service

To configure the Service Framework Time Sync on the Avid System Monitor server:

- Use the Avid Service Configuration tool to configure the Time Sync service in Slave mode to match the system you use to maintain time sync in your network. For additional information, see the *Avid Interplay Software Installation and Configuration Guide*.

3 Installing Software on the Avid System Monitor Server

4 Configuring Monitored Nodes

This chapter describes how to install and configure software on the nodes that are being monitored.

- [Configuring the Windows SNMP Agent](#)
- [Configuring the Interplay Engine](#)
- [Configuring an Interplay Stream Server](#)
- [Configuring the ISIS System Director](#)
- [Configuring a Media Indexer](#)
- [Configuring Additional Servers with the Monitoring Gateway](#)
- [Installing the Avid Monitoring Gateway Service](#)
- [Generating SNMP Traps from a Network Switch](#)

Configuring the Windows SNMP Agent

This section describes how to install the SNMP agents used by the Avid System Monitor system. For a list of systems that require these agents, see [“Software Installation Checklist” on page 25](#) and [“Methods for Discovering Systems to be Monitored” on page 110](#).

Installing and Configuring the Windows SNMP Agent

Before you begin, check whether the SNMP Service is installed on the system.

To check whether the SNMP Service is installed on the system:

1. Right-click My Computer and select Manage.
2. Open Services and Applications and click Services.
3. Scroll down the list of Services and determine whether SNMP Service and SNMP Trap Service are available.
4. Do one of the following:
 - If the Services are not in the list, proceed to [“Installing the SNMP Services” on page 56](#).

4 Configuring Monitored Nodes

- If the Services are in the list, proceed to “Configuring the Microsoft SNMP Agent” on page 58.

Installing the SNMP Services

Before you install the Windows SNMP agent you can determine whether the SNMP agent installer is on the hard drive or whether you must use the Windows DVD that came with your system. Depending on how your Avid system is configured there may an Installables folder on the D drive.

To determine whether the installer is on the system:

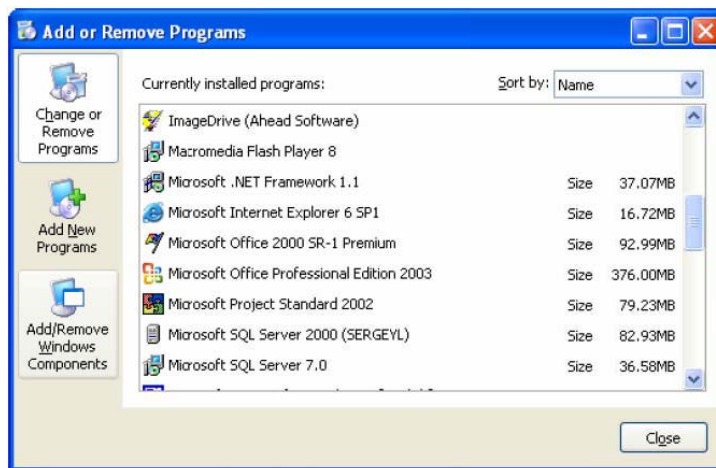
1. If there is a D drive on your system, check for the availability of an Installables folder at the top level of the drive. Some of the Avid Recovery DVDs automatically place this directory on the D drive.
2. If there is an Installables folder, proceed to the following procedure.
3. If there is no Installables folder then you must obtain the Windows DVD for this operating system. Obtain the DVD and proceed with the following procedure.



Before beginning an installation, it is a good idea to collect all of the DVDs that you may need during the installation. See “What to Bring to an Installation” on page 24.

To install the SNMP Services:

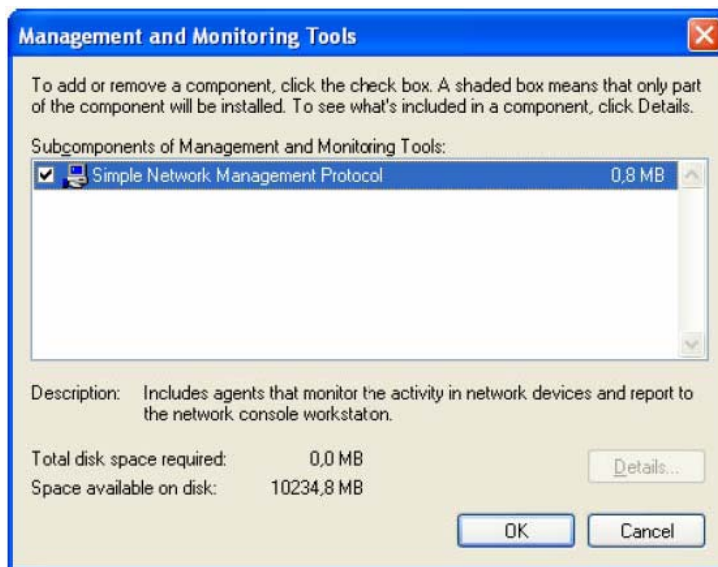
1. Open the Control Panel and double click Add or Remove Programs.



2. Click Add/Remove Windows Components.
3. In the Components window, select Management and Monitoring Tools (but do not select or clear its check box), and then click Details.



4. Select the Simple Network Management Protocol check box, and click OK.



5. If you have an Installables folder on the system, navigate to the following folder and click Next.

32-bit systems: D:\Installables\I386

64-bit systems: D:\Installables\R2\AMD64

4 Configuring Monitored Nodes



You may be prompted for the path twice during the installation. Supply the same path each time.

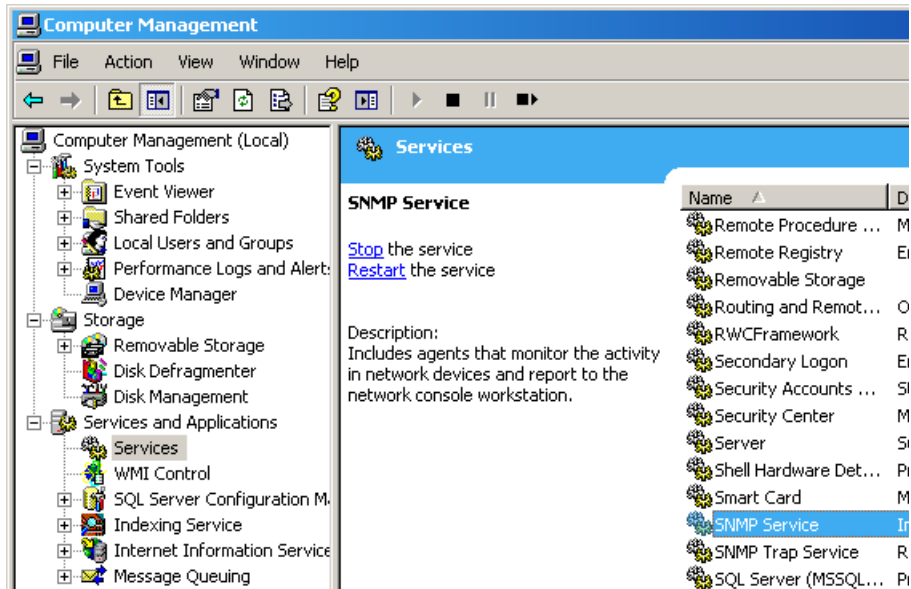
6. If you do not have an Installables folder, insert the system disk and follow the online instructions to install the Simple Network Management Protocol.

Configuring the Microsoft SNMP Agent

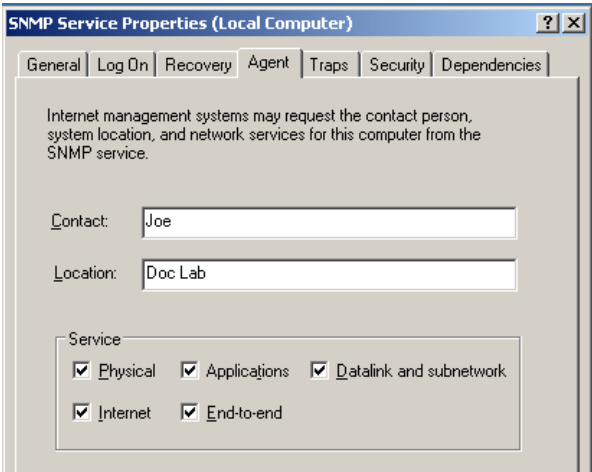
This section describes how to configure the SNMP Service and SNMP Trap Service on a system that will send traps to the Avid System Monitor server.

To configure the Microsoft SNMP agent:

1. Rick-click My Computer and select Manage.
2. Open Services and Applications and click Services.



3. Scroll down the list of Services, right-click SNMP Service, and select Properties.
The SNMP Agent window opens.
4. Click the General tab and select Automatic.
5. Click the Agent tab, select all the check boxes, and (optional) add contact information as shown in the following illustration.

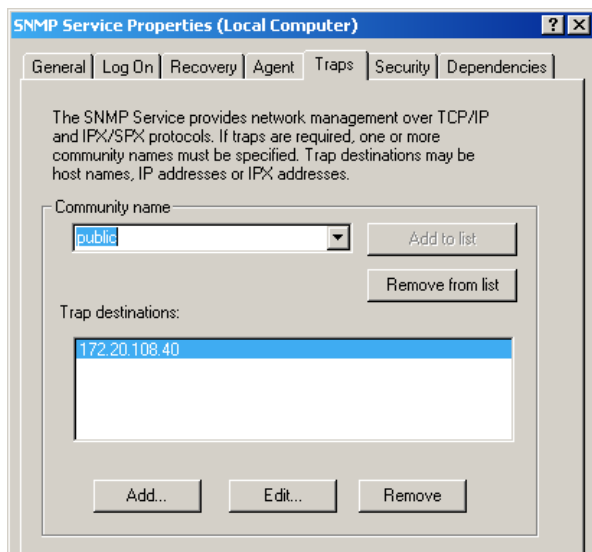


The contact information appears on the OpenNMS interface for that particular node. For example, the following illustration shows information the same contact information displayed in OpenNMS.

SNMP Attributes	
Name	DOCM1
Object ID	.1.3.6.1.4.1.311.1.1.3.1.2
Location	Doc Lab
Contact	Joe
Description	Hardware: x86 Family 15 Model 4 Stepping 1 AT/AT COMPATIBLE - Software: Windows Version 5.2 (Build 3790 Multiprocessor Free)

6. Click the Traps tab and do the following:
 - a. Enter public in the Community name field and click Add to List (the name is case sensitive).
 - b. Click Add in the Trap destination area and add the IP address of the system running the Avid System Monitor software.

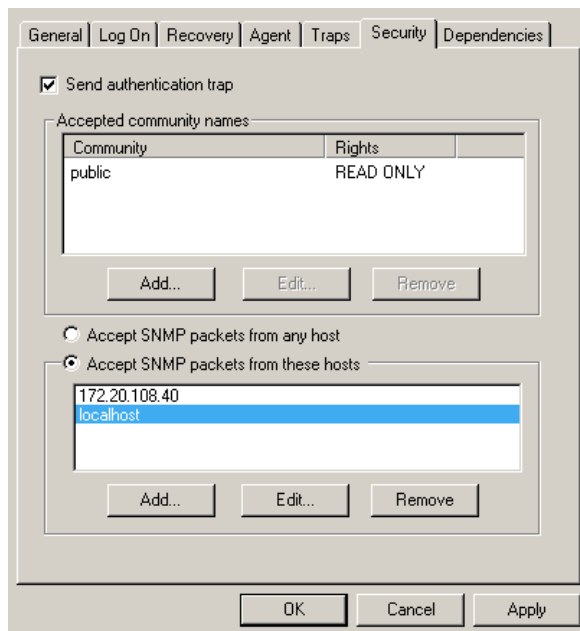
4 Configuring Monitored Nodes



By default, Avid System Monitor expects the “public” community string name value. To use a different name, see “Customizing the SNMP Community String Value” on page 62.

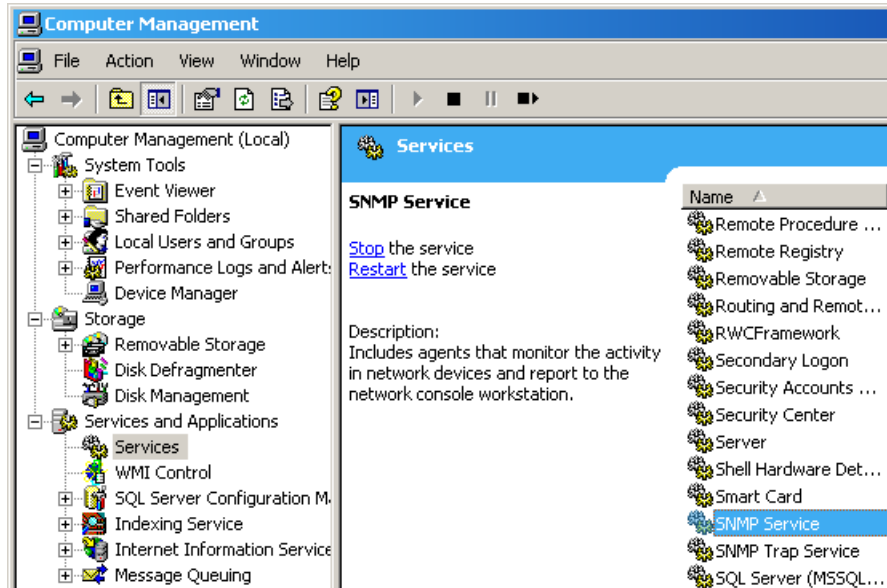
7. Click the Security tab and do the following:
 - a. In the Accepted community name area, click Add, use the default READ ONLY setting and type public (the string is case sensitive).
 - b. Click Accept SNMP packets from these hosts.
 - c. Click Add and enter the IP address of the Avid System Monitor server. Then click OK.

- d. Click Add and type localhost. Then click Add.



8. Click Apply and then click OK to close the SNMP Service dialog box.
9. In the Computer Management window, right-click SNMP Trap Service and select Properties.
10. On the General tab, select Automatic, click Apply, and click OK.
11. In the Computer Management window, select the SNMP Service and click Stop the service and then start or restart the service.

4 Configuring Monitored Nodes



12. Stop the SNMP Trap Service and set it to Manual.

Customizing the SNMP Community String Value

By default, Avid System Monitor expects a value of “public” for the SNMP community string value. For security reasons, some sites prefer to use a custom value. If this is the case at our site you can use a different value for a specific node or for all the nodes within a specific range of IP addresses.

To use a custom community string value:

1. Configure the custom community string values on the individual nodes.
2. Launch the Avid System Monitor application.
3. Click Admin and then click Configure SNMP Community Names by IP.
4. Follow the instructions on the page to change the community string for one node or for all the nodes within a range of IP addresses.

Configuring the Interplay Engine

This section describes how to configure the Interplay Engine to send SNMP traps to Avid System Monitor.



Install the Interplay SNMP agent after you install the Avid Interplay Engine software on the interplay Engine. This is the only way to guarantee that the SNMP agent components are correctly installed and configured.



On a cluster system, install the agent on both nodes.



Ensure that your local firewall does not block port 161. If the port is blocked, the SNMP agent will not respond.

To install the Interplay SNMP agent:

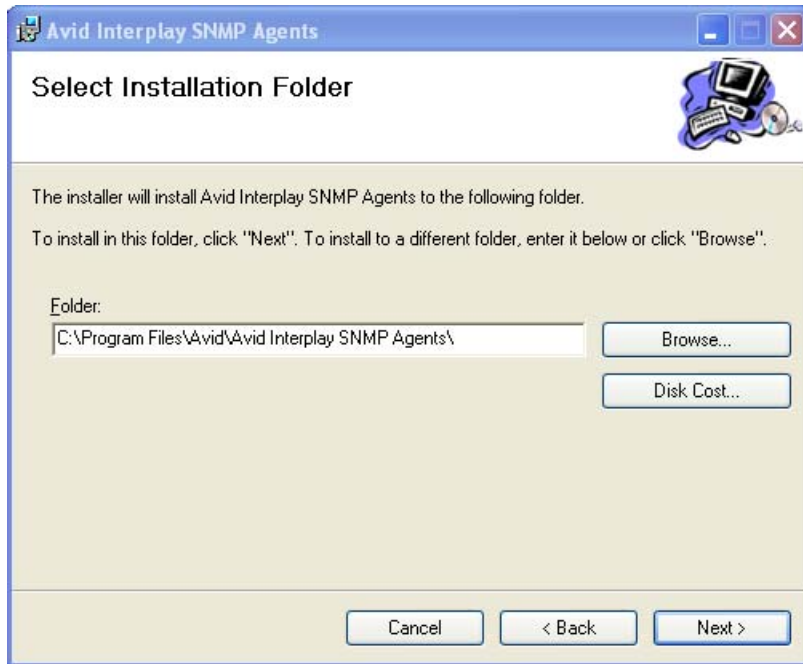
1. Install and configure the Microsoft SNMP agent as described in [“Installing and Configuring the Windows SNMP Agent” on page 55](#).
2. Open the Avid System Monitor installer and click Node Setup.
3. Click Avid Interplay Engine and Stream Server.



If the software is already installed, use the Control Panel to uninstall it before continuing with the install.

4. The Welcome screen opens. Click Next.
The Select Installation folder opens.

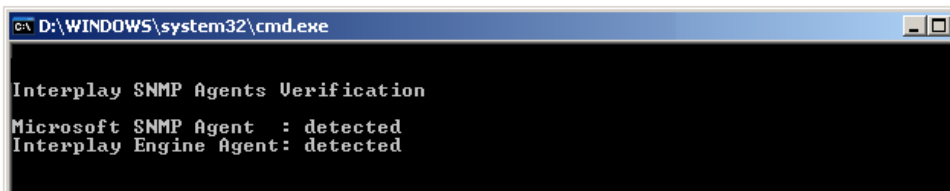
4 Configuring Monitored Nodes



5. Click Next to begin the installation and follow the system prompts to complete the install.

To verify the installation:

1. Open a command prompt window.
2. Navigate to the tools directory in the Interplay SNMP installation directory. For example:
C:\Program Files\Avid\Avid Interplay SNMP Agents\tools
3. Execute the snmptest.cmd. The results should look as shown in the following illustration.



The snmptest.cmd command only works if the community string is public. If you are using a different community string, don't use the verification command at this time.

If you receive an error message, check the Windows eventlog for further troubleshooting steps. Also, ensure that you have restarted the Microsoft SNMP agent as described at the end of the Interplay SNMP Agent installation section.

4. Next, add an SNMP user to the Interplay database as described in the following section.

Adding an SNMP User to the Interplay Database

This section describes how to create an Interplay database user with the following attributes:

- Name: SNMP, password: avid
- Permissions: Read access to the Projects folder.

The Interplay SNMP agent uses this account to test whether it can log into the Interplay database.



The SNMP user can have higher permissions if its convenient. For example, if you are setting up a number of Interplay users at the same time that all have Admin privileges to the entire database, you can set the SNMP user up the same way.

To add an SNMP user to the Interplay database:

1. Start the Interplay Administration tool.
2. In the User Management section of the Interplay Administrator window, click the User Management icon.
The User Management view opens.
3. In the Users pane, select the Everyone group.
4. Click the Create User button.
5. Add the following attributes:
 - Name: SNMP
 - Password: avid (all lowercase)
 - Role: Read only or No Access. Later in this procedure you will grant Read access to the Projects folder.
 - Authentication provider: Internal Authentication
6. Click Apply.
7. On the top left-hand side of the Administration window, click Menu to close the User Management window.

4 Configuring Monitored Nodes

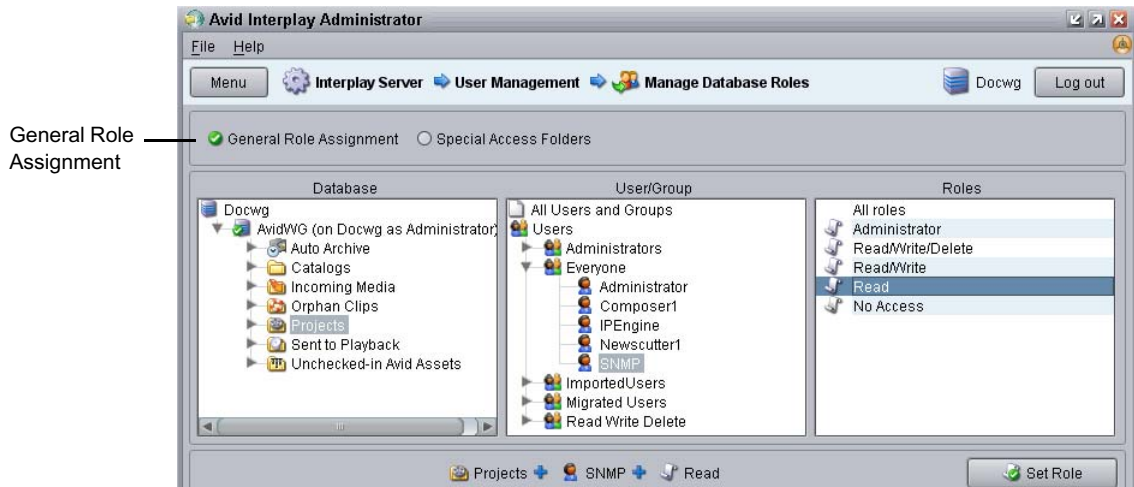
To set the Read only role for the SNMP user:

1. In the User Management section of the Interplay Administrator window, click the Manage Database Roles icon.

The Manage Database Roles view opens.

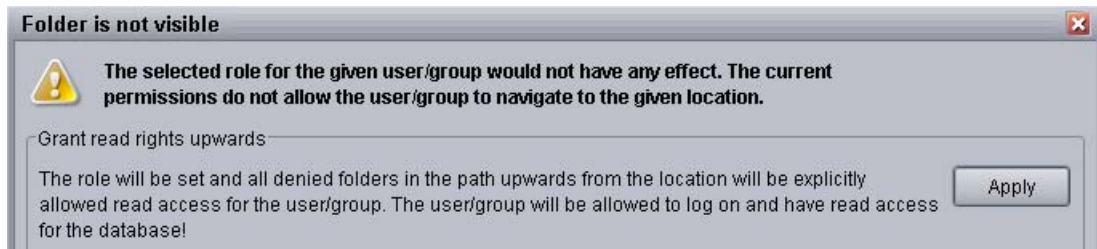
2. Select the General Role Assignment option.
3. In the Database pane, open the Interplay database and select the Projects folder.
4. In the User/Group column, select the SNMP user.
5. In the Roles column, select Read.

The formula in the middle of the view shows your selection. For example, in the following illustration, you are going to give the SNMP user the Read role (read-only access) for the Projects folder.



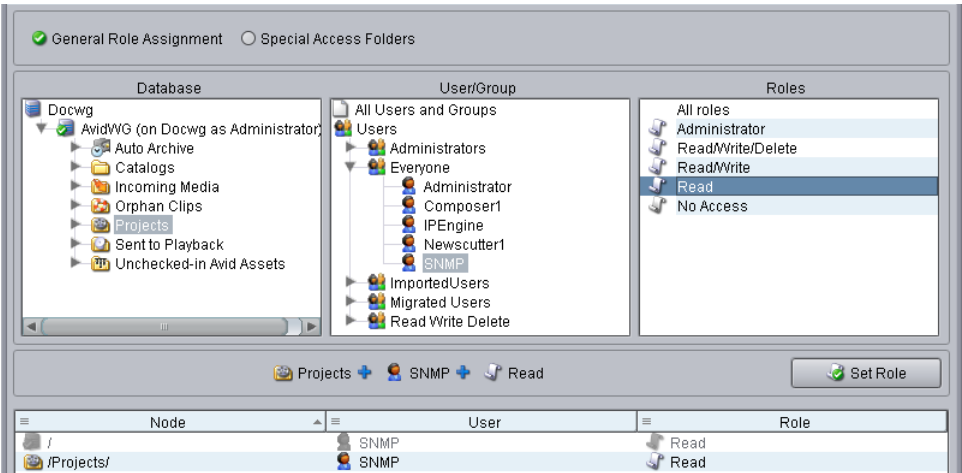
6. Click Set Role.

A dialog box appears asking for you to verify the folder permissions for the user.



7. Click the top selection to allow the user to read down the path.

The role appears in the lower panel.



8. To verify the addition of the user, log into Interplay Access with the SNMP user and avid password.

Using Provisioning Groups to An Add Interplay Engine to OpenNMS

You use provisioning group templates to add the Interplay Engine to OpenNMS. See [“Configuring a Standalone Interplay Engine” on page 84](#) or [“Configuring Cluster Systems” on page 88](#).

Configuring an Interplay Stream Server

Configure an Interplay Stream server just as you would set up an Interplay Engine. Set up SNMP and install the Interplay agent on the Stream Server. The Interplay agent is configured to automatically recognize an Interplay Stream Server.

You use a provisioning group templates to add the Stream Server to OpenNMS. After you configure SNMP and install the Interplay SNMP agent, see [“Configuring an Interplay Stream Server” on page 102](#).

Configuring the ISIS System Director

The following monitoring features are available for ISIS System Directors:

- The ISIS SNMP agent - the agent is automatically installed on ISIS 5000 System Directors and requires installation on ISIS 7000 systems.
- ISIS 7000 and ISIS 5000 both support sending SNMP traps based on the information that the System Director sends to the Windows event log. These are the same events that you can configure to be sent as email notifications from within the ISIS Administrator. You execute the Enable ISIS SNMP Trap Events command from the Avid System Monitor installer to enable this feature.



For a list of events that your ISIS version sends to the Windows Event log, see the section on “E-mail Notifications” in the ISIS Administration Guide for your release. Any events that are sent as ISIS email notifications are also sent to the Windows Event log.

Installing the ISIS SNMP Agent

The following table describes the ISIS SNMP agent installation for different ISIS systems.

ISIS Version	Installation Process
ISIS 5000	Installed automatically when you install the System Director. No separate installation required.
ISIS 7000 v2.0 through 2.3	Use the ISIS SNMP agent on the Avid System Monitor installer. Use Node Setup > Avid ISIS 7000 System Director
ISIS 7000 v2.4 and greater	Use the ISIS SNMP installer in the ISIS System Director installer kit.

Configuring ISIS System Directors

The ISIS System Director has its own MIB and SNMP agent, similar to the way the Interplay Engine uses the Interplay SNMP agent.

To configure the Windows SNMP service on the System Director system:

- Configure the Windows SNMP service on the ISIS System Director the same way that you configure other systems for OpenNMS. For cluster systems, configure the SNMP service on both physical systems. See [“Configuring the Microsoft SNMP Agent” on page 58](#).

To enable SNMP traps on the System Director:

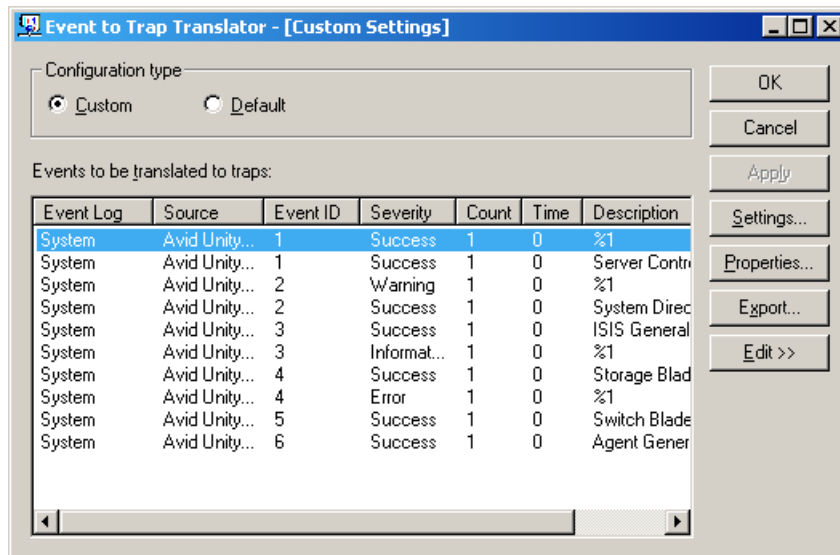
1. Run the Avid System Monitor installer.
2. Click Node Setup.
3. Depending on your System Director, click one of the following:
 - Avid ISIS 7000 System Director
 - Avid ISIS 5000 System Director
4. Click “Enable ISIS SNMP Trap Events.” and wait approximately 30 seconds.



There is no progress bar for this installer and the installer does not provide any feedback that the installer has finished.

5. To verify that the Enable ISIS SNMP Trap Events command executed correctly, use Start > Run and enter the following command in the Run window: **eventwin**.

The system displays the Event to Trap Translator dialog box. If the dialog box is populated as shown in the following illustration, the command ran successfully and the System Director is ready to send SNMP traps to OpenNMS.



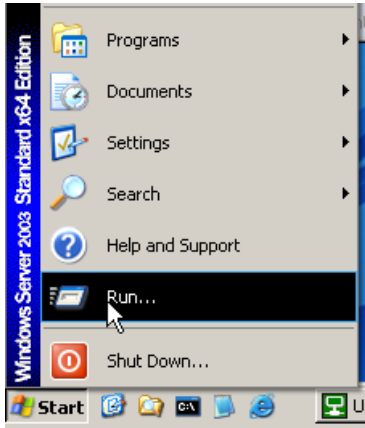
6. Close the installer.
7. On a cluster system, perform the same installation on both physical systems.

For information on testing the Trap notifications, see [“Turning on Notifications and Specifying a Target Email Address” on page 125](#). Also see [“Modifying Notifications from ISIS” on page 161](#).

4 Configuring Monitored Nodes

Identifying a 64-bit Server

A 64-bit server running Windows Server 2003 has an x64 banner along the side of the Start menu as show in the following illustration.



A 64-bit server also has a “Program Files (x86)” directory on the C drive.

Configuring a Media Indexer

You perform the following procedures on a Media Indexer that is monitoring shared storage:

- Configure SNMP. See [“Configuring the Windows SNMP Agent” on page 55.](#)
- Install the Monitoring Gateway service. See [“Installing the Avid Monitoring Gateway Service” on page 73.](#)
- Depending on the version of Media Indexer that is running on the system, you may have to comment out some sections of one of the OpenNMS configuration files.
- Use the Add Interface command in the OpenNMS interface to add the Media Indexer to the set of monitored nodes. See [“Using the Add Interface Command to Add Nodes” on page 112.](#)

Selecting the Software Version of the Media Indexer

OpenNMS polls the Media Indexer system and reads information from the Avid Service Framework Health Monitor. That is where it gets information for resource graphs and threshold values.

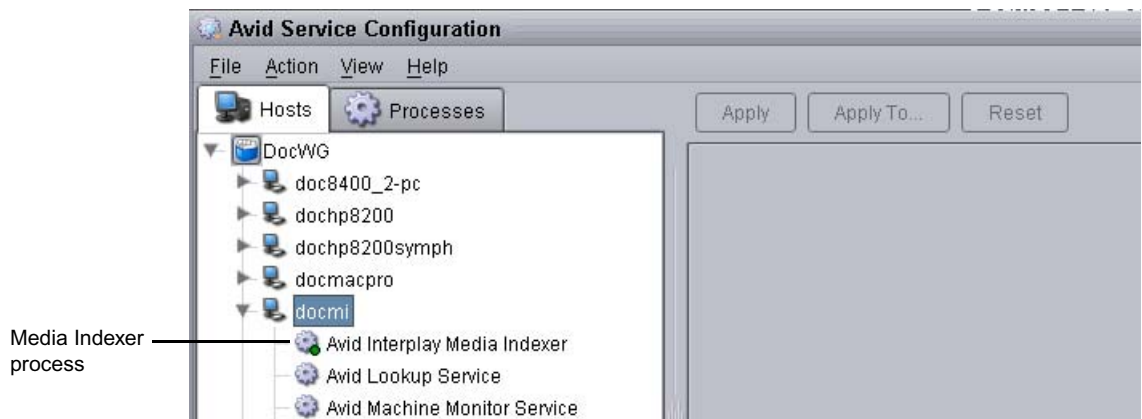
The Media Indexer makes extensive use of the Health Monitor and the values that it sends to the Health Monitor can change from one release to the next. In order to match the values that are collected from one release to the next there are separate sections in the xml file used by OpenNMS to define that values that it collects. The following file contains the values:

Program Files\OpenNMS\etc\http-datacollection-config.xml

There are three sections, for Media Indexer v2.0, v2.1, and v2.2. You comment out the sections that won't be used by adding text to two lines in the section.

To verify the version of the Media Indexer:

1. Open the Avid Service Framework Service Configuration tool and locate the Media Indexer that is monitoring shared storage.
2. Click the triangle to display the Framework processes running on the Media Indexer as shown in the following illustration.



3. Hover the mouse over the Avid Interplay Media Indexer process and the system displays the Media Indexer version number.

To edit the http-datacollection-config.xml file to select the Media Indexer version:

1. If you are running Media Indexer v2.2, there is no need to edit the file. Version v2.2 is set by default.
2. If you are running a version other than v2.2, open the following file in an application like WordPad;

Program Files\OpenNMS\etc\http-datacollection-config.xml

3. Locate the Media Indexer sections. For example, the section in the following illustration is used for Media Indexer v2.0.

4 Configuring Monitored Nodes

```
</http-collection>
<!-- This is the configuration block for 2.0 of the Avid Media Inde>
<!-- This is not the default Media Indexer schema - to use this sche
<!-- in this list to "AvidInterplayMediaIndexerXX" (where XX is the
<http-collection name="AvidInterplayMediaIndexer20">
  <rrd step="60">
    <rra>RRA:LAST:0.5:1:2880</rra>
    <rra>RRA:AVERAGE:0.5:5:8928</rra>
    <rra>RRA:AVERAGE:0.5:60:8784</rra>
    <rra>RRA:MIN:0.5:60:8784</rra>
    <rra>RRA:MAX:0.5:60:8784</rra>
  </rrd>
  <uris>
    <uri name="AvidInterplayMediaIndexer20">
      <url path="/avidinterplaymediaindexer.snapshot
        port="56002"
```

The text 20 comments out this entire section

Notice that the lines starting with “<http-collection>” and “<url name=’Avid’” have the text “20” as part of the variable name. This effectively comments out the Interplay Media Indexer v2.0 section. Also notice that the commented lines at the top of the section identify this as the v2.0 section.

4. For the section you want to use, remove the numbers at the end of the strings (in this case remove both instances of 20. Don’t remove the quote at the end of the string.
5. Check the other Media Indexer sections and add numbers to the end of the corresponding strings to comment those sections out.

Configuring Additional Servers with the Monitoring Gateway

For this release, the following systems are monitored via the Monitoring Gateway:

- Interplay Media Indexer
- AirSpeed Multi Stream v1.8.1 or higher
- Interplay Capture
- System running the Lookup Service (do not install on the Interplay Engine).

Perform the following procedures on these servers:

- Configure SNMP. See [“Configuring the Windows SNMP Agent” on page 55](#).
- Install the Monitoring Gateway service. See [“Installing the Avid Monitoring Gateway Service” on page 73](#).
- If the system is a Media Indexer monitoring shared storage. see [“Configuring a Media Indexer” on page 70](#).
- Use the Add Interface command in the OpenNMS interface to add the system to the set of monitored nodes. See [“Using the Add Interface Command to Add Nodes” on page 112](#).

Installing the Avid Monitoring Gateway Service

For this release, you can install the Avid Monitoring Gateway on the following systems:

- Interplay Media Indexer
- AirSpeed Multi Stream v1.8.1 or higher
- Interplay Capture
- System running the Lookup Service (do not install on the Interplay Engine).

You must also configure SNMP on these systems. See [“Configuring the Windows SNMP Agent” on page 55](#). For additional information, see [“Methods for Discovering Systems to be Monitored” on page 110](#).



The Monitoring Gateway service runs with earlier versions of the Avid Service Framework.

To install Avid Monitoring Gateway service:

1. Open the Avid System Monitor installer and click Node Setup.
2. Click “Avid Media Indexer, Lookup Service, and Capture and AirSpeed Multi Stream.
3. Click Avid Monitoring Gateway Service.
4. Follow the onscreen prompts and accept the defaults.



If the system displays an error that the Avid Service Framework must be installed first, run the AvidMonitoringGateway installer directly from the Installer\AvidMonitorGateway folder.

5. To verify that the service was installed, start the Avid Service Framework Workgroup Properties tool, click Advanced, and check for the existence of the Avid Monitoring Gateway service.

Monitoring Gateway in the Service Configuration Tool

When you run the Avid Service Framework Service Configuration tool, you will notice the Avid Monitoring Gateway service is displayed on the node its running on. The service has its own set of parameters. You do not have to configure anything in the Monitoring Gateway section of the Service Configuration tool.

Generating SNMP Traps from a Network Switch

This section describes how to configure a Cisco switch or a Foundry switch to send SNMP traps to the Avid System Monitor system and how to add a node for the switch in Avid System Monitor.



This section assumes that you have experience configuring switches. If you are not familiar with the process, see your site administrator. Note that some sites have specific requirements regarding configuring switches and may not want them to be monitored by the Avid System Monitor. Check with your site administrator before you configure any switches.

Configuring a Cisco Switch

This section describes how to configure SNMP on a Cisco switch. The following table shows the commands that you use. Values in italics represent variables that may be specific to the site configuration.

Command	Description
<code>access-list <i>1</i> permit <i>172.20.110.19</i></code>	Configure the IP address that is allowed to connect to the switch via SNMP. This will be the IP address of the Avid Monitor Service server. The access list number can be anything from 1-99 but be sure to check the configuration prior to configuring an access list and do not use a number already in use.
<code>snmp-server community <i>public</i> RO <i>1</i></code>	Configure the SNMP community string with read-only access and specify the access list number used in the prior step.
<code>snmp-server trap-source <i>Vlan110</i></code>	Configure the interface the switch will use when sending trap messages to the Avid Monitor Service server. For switches with multiple layer-3 interfaces, the trap-source interface should be on the same vlan as the Avid Monitor Service server or the interface that has the optimal routing path to the Avid Monitor Service server.
<code>snmp-server enable traps</code>	Enable SNMP traps for all supported notifications.

Command	Description
<code>snmp-server host 172.20.110.19 version 2c public</code>	Specifies the host IP address of the Avid Monitor Service server to send traps and the version of SNMP to use.
<code>no snmp trap link-status</code>	Suppress up/down trap notifications on a per interface basis.

The following illustration shows sample output from a telnet session while configuring the first five parameters from the table.

```

CA: Telnet 172.20.110.10
wgeng-4948-01#
wgeng-4948-01#conf t
Enter configuration commands, one per line. End with CNTL/Z.
wgeng-4948-01(config)#access-list 1 permit 172.20.110.19
wgeng-4948-01(config)#snmp-server community public RO 1
wgeng-4948-01(config)#snmp-server trap-source Vlan110
wgeng-4948-01(config)#snmp-server enable traps
wgeng-4948-01(config)#snmp-server host 172.20.110.19 version 2c public
wgeng-4948-01(config)#exit
wgeng-4948-01#wr mem
Building configuration...
Compressed configuration from 7882 bytes to 2591 bytes[OK]
wgeng-4948-01#

```

The following shows the sample telnet session. Commands are in bold. Supply the IP address of your own OpenNMS server. Use the “show run” command to display the current settings. In this example, the IP address of the OpenNMS server is 172.20.110.19.

telnet <IP address of the switch>

<login information>

enable

wgeng-4948-01#

wgeng-4948-01#**conf t**

Enter configuration commands, one per line. End with CNTL/Z.

wgeng-4948-01(config)#**access-list 1 permit 172.20.110.19**

wgeng-4948-01(config)#**snmp-server community public RO 1**

wgeng-4948-01(config)#**snmp-server enable traps**

wgeng-4948-01(config)#**snmp-server host 172.20.110.19 version 2c public**

wgeng-4948-01(config)#**exit**

wgeng-4948-01#**wr mem**

Building configuration...

Compressed configuration from 7882 bytes to 2591 bytes[OK]

wgeng-4948-01#

Disabling Trap Notification for Specific Cisco Interfaces

For some interfaces on a switch, it may be desirable to not receive trap notifications on up/down status. To suppress trap notifications on a per interface basis, log into the switch and execute the following command within each interface configuration mode.

```
wgeng-4948-01#conf t
Enter configuration commands, one per line. End with CNTL/Z.
wgeng-4948-01(config)#int gi1/1
wgeng-4948-01(config-if)#no snmp trap link-status
wgeng-4948-01(config-if)#exit
wgeng-4948-01(config)#exit
wgeng-4948-01#
```

Configuring a Foundry Switch

This section describes how to configure SNMP on a Foundry switch. The following table shows the commands that you use. Values in *italics* represent variables that may be specific to the site configuration.

Command	Description
snmp-client <i>172.20.110.19</i>	Configure the IP address that is allowed to connect to the switch via SNMP. This will be the IP address of the Avid Monitor Service server.
snmp-server community <i>public</i> RO	Configure the SNMP community string with read-only access.
snmp-server trap-source <i>ve 110</i>	Configure the interface the switch will use when sending trap messages to the Avid Monitor Service server. For switches with multiple layer-3 interfaces, the trap-source interface should be on the same vlan as the Avid Monitor Service server or the interface that has the optimal routing path to the Avid Monitor Service server.
snmp-server host <i>172.20.110.19</i> version v2c <i>public</i> (supported on foundry code 4.x and above)	Specifies the host IP address of the Avid System Monitor server to send traps and the version of SNMP to use.
snmp-server host <i>172.20.110.19</i> <i>public</i> (no version to specify on Foundry code below 4.x)	
no snmp-server enable traps link-change	Suppress up/down trap notifications on a per interface basis.



All supported SNMP trap notifications are enabled by default on a Foundry switch.

The following shows the sample telnet session using the first four parameters from the table. Commands are in bold.

```
telnet@wgeng-FESX-01>en
Password:
telnet@wgeng-FESX-01#conf t
telnet@wgeng-FESX-01(config)#snmp-client 172.20.110.19
telnet@wgeng-FESX-01(config)#snmp-server community public RO
telnet@wgeng-FESX-01(config)#snmp-server trap-source ve 110
telnet@wgeng-FESX-01(config)#snmp-server host 172.20.110.19 version v2c public
telnet@wgeng-FESX-01(config)#exit
telnet@wgeng-FESX-01#wr mem
Write startup-config done.
telnet@wgeng-FESX-01#
```

Disabling Trap Notification for Specific Foundry Interfaces

For some interfaces on a switch, it may be desirable to not receive trap notifications on up/down status. To suppress trap notifications on a per interface basis, log into the switch and execute the following command within each interface configuration mode.

```
telnet@wgeng-FESX-01#
telnet@wgeng-FESX-01#conf t
telnet@wgeng-FESX-01(config)#interface ethernet 1
telnet@wgeng-FESX-01(config-if-e1000-1)#no snmp-server enable traps link-change
telnet@wgeng-FESX-01(config-if-e1000-1)#exit
telnet@wgeng-FESX-01(config)#exit
telnet@wgeng-FESX-01#wr mem
Write startup-config done.
telnet@wgeng-FESX-01#
```

Configuring a Force10 Switch

This section describes how to configure SNMP on a Force10 switch. The Force10 is used by ISIS 5000 systems. The following table shows the commands that you use. Values in *italics* represent variables that may be specific to the site configuration.

Command	Description
<code>snmp-server community <i>public</i> ro</code>	Configure the SNMP community string with read-only access.
<code>snmp-server host <i>10.105.228.29</i> traps version 2c</code>	Specifies the host IP address of the Avid System Monitor server to send traps and the version of SNMP to use.
<code>snmp-server enable traps</code>	Specify which traps the Force10 system sends to the trap receiver (Avid System Monitor server).
<code>no snmp trap link-status</code>	Suppress up/down trap notifications on a per interface basis

The following shows a sample telnet session run n a Force10 switch to enable SNMP monitoring and traps. Commands are in bold. Supply the IP address of your own OpenNMS server.

```
telnet <IP address of the switch>
<login information>
enable
ISIS_Force10#conf t
ISIS_Force10(conf)#snmp-server community public ro
ISIS_Force10(conf)#snmp-server host 10.105.228.29 traps version 2c
ISIS_Force10(conf)#snmp-server enable traps
ISIS_Force10(conf)#exit
ISIS_Force10#
```

Disabling Trap Notification for Specific Force10 Interfaces

For some interfaces on a switch, it may be desirable to not receive trap notifications on up/down status. For example, you may not want to receive alerts every time an editor system reboots. To suppress trap notifications on a per interface basis, log into the switch and execute the following command within each interface configuration mode.

```
sw-wgeng-F10#conf t
sw-wgeng-F10(conf)#int gi0/9
sw-wgeng-F10(conf-if-gi-0/9)#no snmp trap link-status
sw-wgeng-F10(conf-if-gi-0/9)#exit
sw-wgeng-F10(conf)#
```

Using Add Interface to Add a Network Switch to OpenNMS

To add the switch as a node on the Avid System Monitor system:

1. Open the Avid System Monitor interface and click Admin.
2. Click Add Interface in the Nodes area.
3. Enter the IP address of the switch and click Add.
4. To view the node, click Node List and select the system you added. Notice that OpenNMS uses the fully qualified domain name for the switch.

Configuring Data Collection for a Network Switch

By default, OpenNMS only collects data on the primary interface for a switch. This section describes how to instruct OpenNMS to collect data about all the interfaces.

4 Configuring Monitored Nodes

To collect data on all interfaces for a switch:

1. Locate the node in the node list (or search for it) and open the node page.

The following illustration shows the node details view for a Cisco switch.

Admin button

Home / Search / Node
Node: sw-4948-war02
View Events View Alarms View Outages Asset Info Resource Graphs Rescan **Admin** Schedule Outage

SNMP Attributes

Name	sw-war02
Object ID	.1.3.6.1.4.1.9.1.659
Location	
Contact	
Description	Cisco IOS Software, Catalyst 4000 L3 Switch Software (cat4000-I9S-M), Version 12.2(25)EWA8, RELEASE SOFTWARE (fc1)..Technical Support: http://www.cisco.com/techsupport..Copyright (c) 1986-2007 by Cisco Systems, Inc...Compiled Wed 24-Jan-07 14:38 by pwade

General (Status: Active)

View Node Bridge/STP Info
View Node Link Detailed Info

Surveillance Category Membership

LAN Gateways
Warroom Lab

Notification

You: Outstanding: (Check)
You: Acknowledged: (Check)

Recent Events

☐ 617042	9/5/11 20:08:38
☐ 578080	9/4/11 20:02:05
☐ 538854	9/3/11 19:54:58
☐ 499545	9/2/11 19:47:48
☐ 460100	9/1/11 19:40:47

Availability

Availability (last 24 hours)	100.000%	
10.106.128.2	Overall	100.000%
	ICMP	100.000%
	SNMP	100.000%
	StrafePing	100.000%
10.106.129.2	Overall	100.000%
	ICMP	100.000%
	SNMP	100.000%

2. Click Admin and then click “Configure SNMP Data Collection per interface.”

The following illustration shows a portion of the interfaces that are monitored by the node.

Home / Admin / Select SNMP Interfaces

Choose SNMP Interfaces for Data Collection

Listed below are all the interfaces discovered for the selected node. If snmpStorageFlag is set to "select" for a collection scheduled below will have their collected SNMP data stored. This has no effect if snmpStorageFlag is set to "primary" or "all". In order to change what interfaces are scheduled for collection, simply click the collect column and a combobox will appear. Note: Interfaces marked as Primary or Secondary will always be selected for data collection. To remove them, edit the IP address.

Node ID: 62
Node Label: sw-4948-war01

Index	IP Address	SNMP ifType	SNMP ifDescr	SNMP ifName
60	10.106.128.1	53	Vlan128	Vl128
61	10.106.129.1	53	Vlan129	Vl129
62	10.106.130.1	53	Vlan130	Vl130
49	10.106.191.2	6	GigabitEthernet...	Gi1/48
51	0.0.0.0	6	TenGigabitEther...	Te1/50
52	0.0.0.0	1	Null0	Nu0
53	0.0.0.0	53	Vlan1	Vl1
54	0.0.0.0	53	unrouted VLAN 1	VLAN-1

- On the far right of the window under the Collect heading, select any interfaces that you do not want to monitor as shown in the following illustration.

Home / Admin / Select SNMP Interfaces

Choose SNMP Interfaces for Data Collection

Listed below are all the interfaces discovered for the selected node. If snmpStorageFlag is set to "select" for a collection scheduled below will have their collected SNMP data stored. This has no effect if snmpStorageFlag is set to "primary" or "all". In order to change what interfaces are scheduled for collection, simply click the collect column and a combobox will appear. Note: Interfaces marked as Primary or Secondary will always be selected for data collection. To remove them, edit the IP address.

Node ID: 62
Node Label: sw-4948-war01

Collect
Collect
Collect
Collect
Collect
Collect
Collect
Collect
Don't Collect
Default
Collect

4 Configuring Monitored Nodes

To test the SNMP trap generation:

- ▶ Remove a network cable from the switch, wait a few seconds, and then plug it back in. You should see link-up and link-down events in the Recent Event column as shown in the following illustration.



After you add a node, it could take as long as 20 minutes before events start appearing in the Avid System Monitor interface.

Recent Events			
☐ 49895	3/25/09 16:47:00	Normal	Agent Interface Down (linkUp Trap) on interface index:11; ifDescr: ethernet11; ifName;; IfAlias:
☐ 49891	3/25/09 16:46:54	Minor	Agent Interface Down (linkDown Trap) on interface index:11; ifDescr: ethernet11; ifName;; ifAlias:
☐ 49415	3/25/09 15:46:08	Minor	InterplayEngine outage identified on interface 172.20.54.38 with reason code: SNMP poll failed, addr=172.20.54.38 oid=.1.3.6.1.4.1.526.10.1.1.0.
☐ 49414	3/25/09 15:46:00	Normal	A services scan has been completed on this node.
☐ 49413	3/25/09 15:46:00	Normal	Polling will begin/resume for InterplayEngine service on interface 172.20.108.65.

To remove discovered services from a switch interface in OpenNMS:

- ▶ It is often useful to remove some of the discovered services from a switch. See [“Removing Discovered Services from a Node” on page 173.](#)

5 Working with Provisioning Groups

This chapter contains the following topics:

- [Overview of Provisioning Groups](#)
- [Configuring a Standalone Interplay Engine](#)
- [Configuring Cluster Systems](#)
- [Interplay Engines and ISIS v2.3 and v2.4](#)
- [Using Provisioning Groups to Configure an ISIS 7000 System Director](#)
- [Configuring an Interplay Stream Server](#)
- [Defining Nodes with Basic Up/Down Status](#)
- [Creating New Provisioning Groups](#)

Overview of Provisioning Groups

There are two basic ways to configure systems in an OpenNMS environment:

- Automatic discovery to discover all of the services running on a node. Use the Add Interface command to configure automatic discovery.
- Provisioning groups: this feature allows you to specify which services are going to be monitored on a node. This simplifies the monitoring process and allows you to monitor only the recommended services.

Avid supplies a number of provisioning group templates. This chapter describes how to use the templates and how to create new provisioning groups.

For a description of the features that are new for Provisioning Groups in Avid System Monitor v1.2.1, see [“Changes to Provisioning Groups” on page 32](#).

Determining Which Provisioning Group Template to Use

There are specific templates for the different types of nodes that will be monitored. See [“Methods for Discovering Systems to be Monitored” on page 110](#).

Configuring a Standalone Interplay Engine

This section describes how to use the IPE-standalone template to configure a standalone Interplay Engine. For cluster systems, see [“Configuring Cluster Systems” on page 88](#).

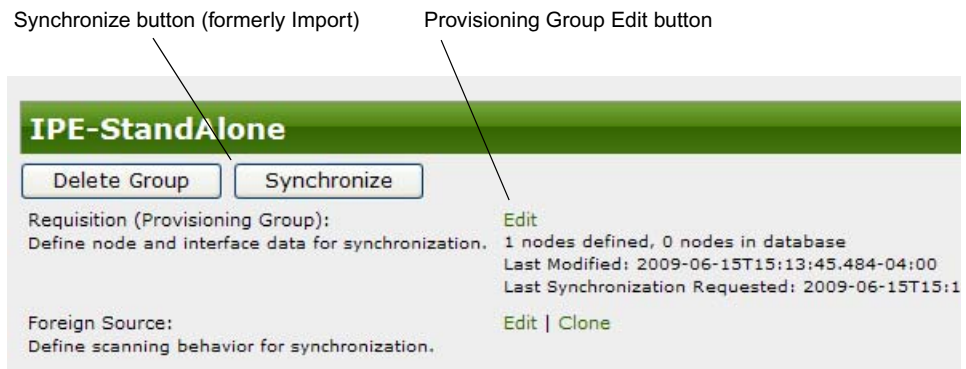


If you have already configured the Interplay Engine using automatic discovery, use Admin > Delete Nodes to delete the Interplay Engine from the OpenNMS database, restart OpenNMS, and then add it back into OpenNMS using the provisioning group template.

To enter values into the IPE-standalone template:

1. Click the Admin link in OpenNMS.
2. Under the Nodes section, click Manage Provisioning Groups.

The Provisioning Groups window opens. The following illustration shows the IPE-Standalone section. When you first start to configure the node it shows 1 node defined, 0 nodes in the database. This means that the information in the template is not associated with any nodes in the OpenNMS database.



3. Click the Edit button to access the provisioning group values. The following illustration shows the default template with a default name and IP interfaces. FQDN stands for “fully qualified domain name.”

Home / Admin / Provisioning Groups / Edit Requisition

Manually Provisioned Nodes for Group: IPE-StandAlone

Done Add Node

- Node node1.FQDN ForeignId 1244473588312 Site IPE
 - IP Interface 1.1.2.1 Description node-1 Right SNMP
 - Service AvidISISClient
 - Service AvidInterplayEngine
 - Service Win32AvidWGPreviewServer
 - Service Win32AvidWGTCPCOMBridge
 - Service Win32AvidWorkgroupVSSService
 - Service Win32AvidWGServerBrowser
 - Service Win32Time
 - Service Win32Server
 - Service Win32NetLogon
 - Service Win32AvidUnityISISClientAgent
 - Service Win32AvidFosFS
 - Service SNMP
 - Service StrafePing
 - Service ICMP
 - IP Interface 1.1.1.1 Description node-1 Left SNMP
 - Service AvidISISClient

- Click the Edit button for the top level Node and type in the fully qualified domain name of the Interplay Engine.

Home / Admin / Provisioning Groups / Edit Requisition

Manually Provisioned Nodes for Group: IPE-StandAlone

Done Add Node

Edit button

Domain name

IP address

- Node b3-eng2.global.avidww ForeignId 1244473588312 Site IPE
 - IP Interface 10.104.100.5 Description node-1 Right
 - Service AvidUnityISISClient
 - Service AvidInterplayEngine

5 Working with Provisioning Groups

5. Click Save at the right end of the line.
6. Click the Edit button for the first IP Interface.
7. Enter the IP address for the right side interface and click Save.
8. Scroll down and click the Edit button for the left side interface.
9. Enter the IP address for the left side interface and click Save.
10. Click Done.

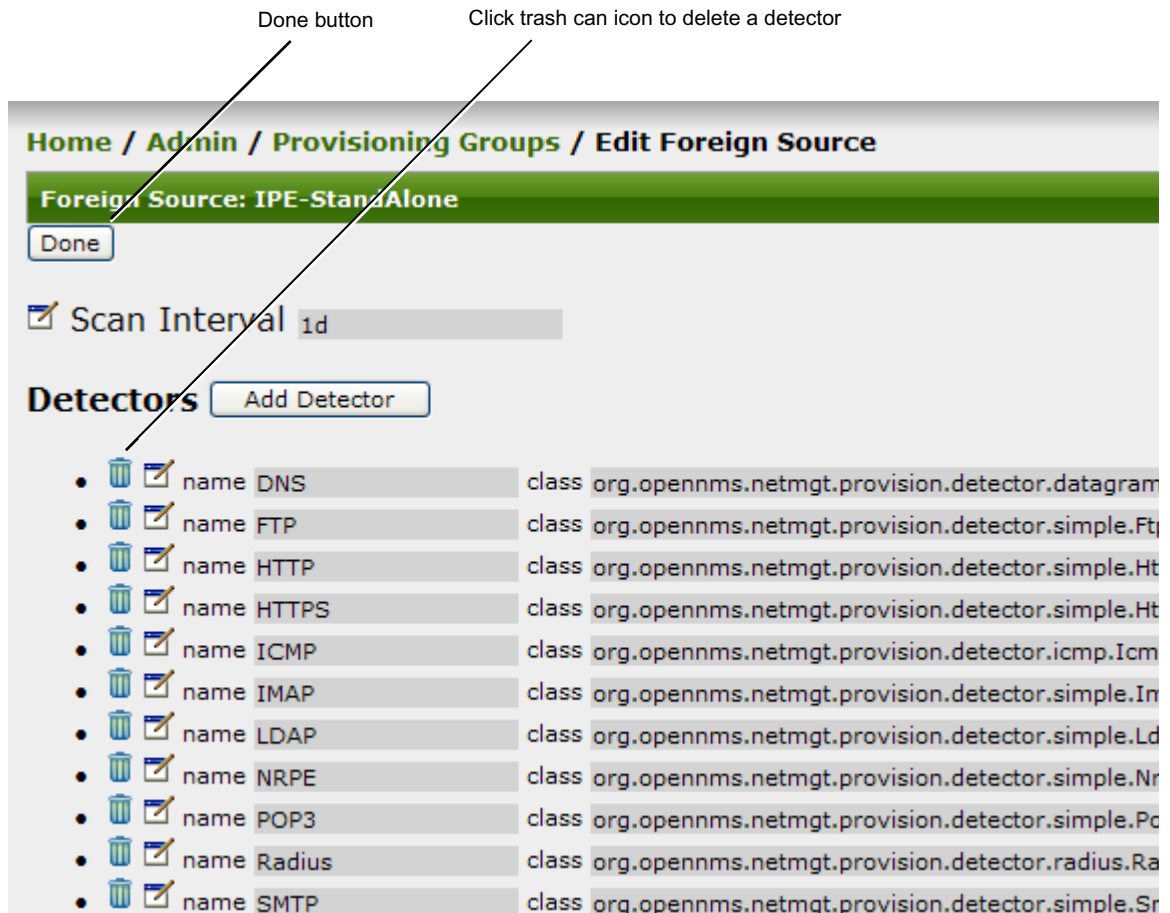
OpenNMS v1.8.10 adds a number of default service monitoring items called detectors to each provisioning group. These detectors are not needed by Avid System Monitor and must be deleted from the provisioning group interface. The following procedure describes how to delete the detectors.

To delete the detectors in a Provisioning Group:

1. Click the Foreign Source Edit button



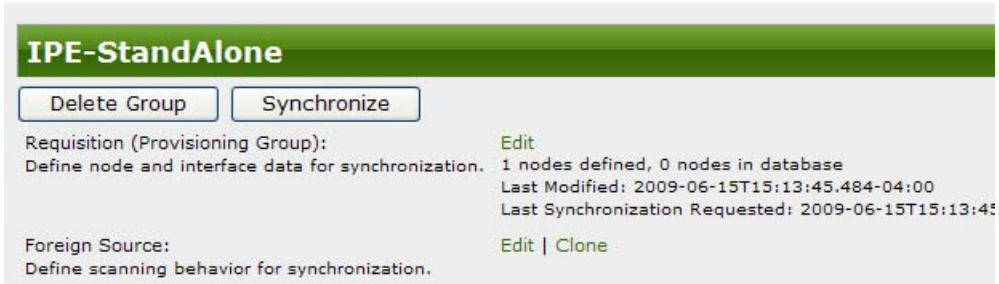
The Foreign Source editing window opens.



2. Click each trash can icon and delete all of the detectors on the page.
3. Click Done.

To instruct OpenNMS to use the updated provisioning group file:

- Click the Synchronize button for the IPE-Standalone provisioning group name.



The screenshot shows the 'IPE-StandAlone' provisioning group configuration page. At the top, there is a green header with the title 'IPE-StandAlone'. Below the header, there are two buttons: 'Delete Group' and 'Synchronize'. The main content area is divided into two sections. The first section is titled 'Requisition (Provisioning Group):' and contains the text 'Define node and interface data for synchronization.' To the right of this text, there is an 'Edit' link. Below this, there is a status line: '1 nodes defined, 0 nodes in database'. The second section is titled 'Foreign Source:' and contains the text 'Define scanning behavior for synchronization.' To the right of this text, there are 'Edit' and 'Clone' links. At the bottom right, there are two lines of text: 'Last Modified: 2009-06-15T15:13:45.484-04:00' and 'Last Synchronization Requested: 2009-06-15T15:13:45.484-04:00'.

OpenNMS imports the template, adds the nodes to OpenNMS, and displays the date of the import in the Last Synchronize Request and Last Changed columns.



It might take a few minutes for the node to appear in the Node List.

Critical Alarms When First Adding an Interplay Engine

During the first few minutes after adding an Interplay Engine to OpenNMS, the system typically displays a number of critical alarms. The following are some examples:

- SNMP user can't log into the Interplay database
- Problem with the number of objects loaded in the Interplay database

These problems are related to the SNMP agent throwing alarms before the system is completely registered with OpenNMS and can usually be ignored. Check back on the Interplay Engine after 20 minutes or so and see if the errors are still occurring. If not, you can ignore those alarms.

Configuring Cluster Systems

This section applies to Interplay Engine and Avid Unity ISIS cluster systems. You should perform these steps on a cluster before you start the Discovery process described in [“Configuring Discovery and the Dashboard” on page 109](#).

You use an Provisioning Groups to configure cluster nodes. Provisioning Groups allow you to add specific nodes and services to OpenNMS without using the automatic Discovery feature. This is useful in the case of a cluster because you need to identify a virtual node that will run the cluster services. The virtual node shows that the cluster services are running regardless of which physical node in the cluster is acting as the primary node.

Avid provides several template files to make it easy to define the nodes in a provisioning group. To configure the template you need to supply the qualified domain name and IP addresses of the virtual node and the two physical nodes in the cluster. The following cluster templates are supplied as part of the custom Avid configuration files.

- IPE-dualNIC
- IPE-singleNIC
- ISIS-SD

The two IPE templates are for dual connected or single connected Interplay Engine clusters. Zone 1 or Zone 2 Interplay Engine clusters are typically dual connected. Zone 3 systems are typically single connected using a redundant network switch. There is only one ISIS template because ISIS clusters are always dual connected.

Sites typically have a spreadsheet or other document that identifies the IP addresses and domain names of servers in the Interplay environment. The following table shows the IP addresses and names used in this section as an example. The Interplay Engine cluster in this example is dual connected as a Zone 2 ISIS client.

VLAN-10	Domain Name (avid-warroom.com)	VLAN 20	Description
10.106.128.4	WARRM-ISIS	10.106.129.4	Virtual ISIS name
110.106.128.5	WARRM-SD1	10.106.129.5	SD cluster node 1
10.106.128.6	WARRM-SD2	10.106.129.6	SD cluster node 2
10.106.128.7	WARRM-IPCLUSTER		Cluster service
10.106.128.8	WARRM-IPE1	10.106.129.8	Cluster node 1
10.106.128.9	WARRM-IPE2	10.106.129.9	Cluster node 2
10.106.128.10	WARRM-MSDTC		MSDTC service
10.106.128.11	WARRM-WKGRP-SVR	10.106.129.11	Virtual Interplay Engine server name

Determine which is the right and left side of the network so you can consistently add values to the template. In this example VLAN-10 is on the left.

Using Provisioning Groups to Configure an Interplay Engine Cluster

Use the following procedures to configure an Interplay Engine cluster.

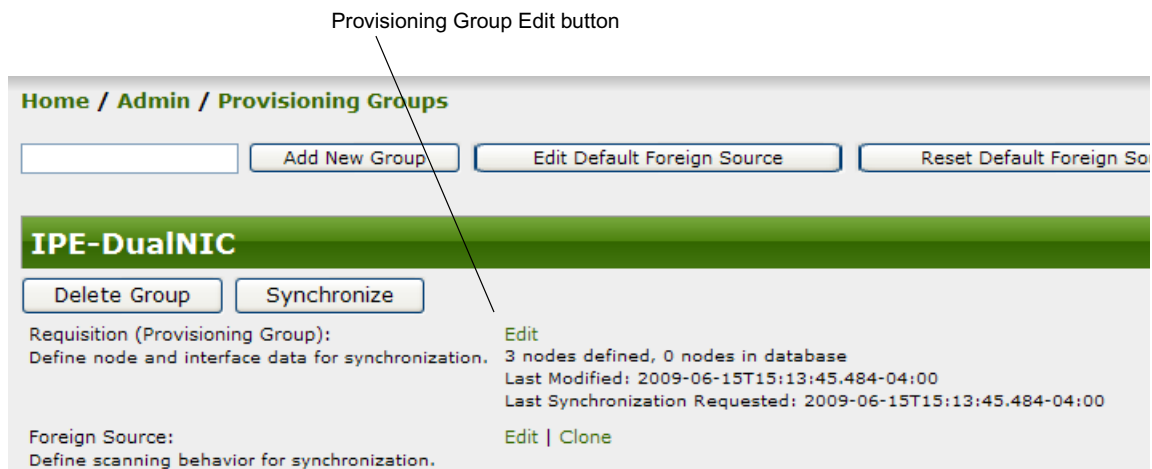
To select the template for the Interplay Engine Provisioning Group:

1. Determine whether your Interplay Engine cluster is single or dual connected and obtain the list of qualified domain names and IP addresses as shown in the table in the previous section.
2. Launch the OpenNMS interface and click the Admin link.
3. In the Nodes area, select Manage Provisioning Groups.

The following two cluster templates are available:

- IPE-DualNIC
- IPE-SingleNIC

The following illustration shows the top level view for IPE-DualNIC.



Do not click Synchronize until you are finished editing the group. If you do, OpenNMS will add an incomplete node definition to the database and you will need to delete the node using Admin > Nodes > Delete Node and then complete the template editing.

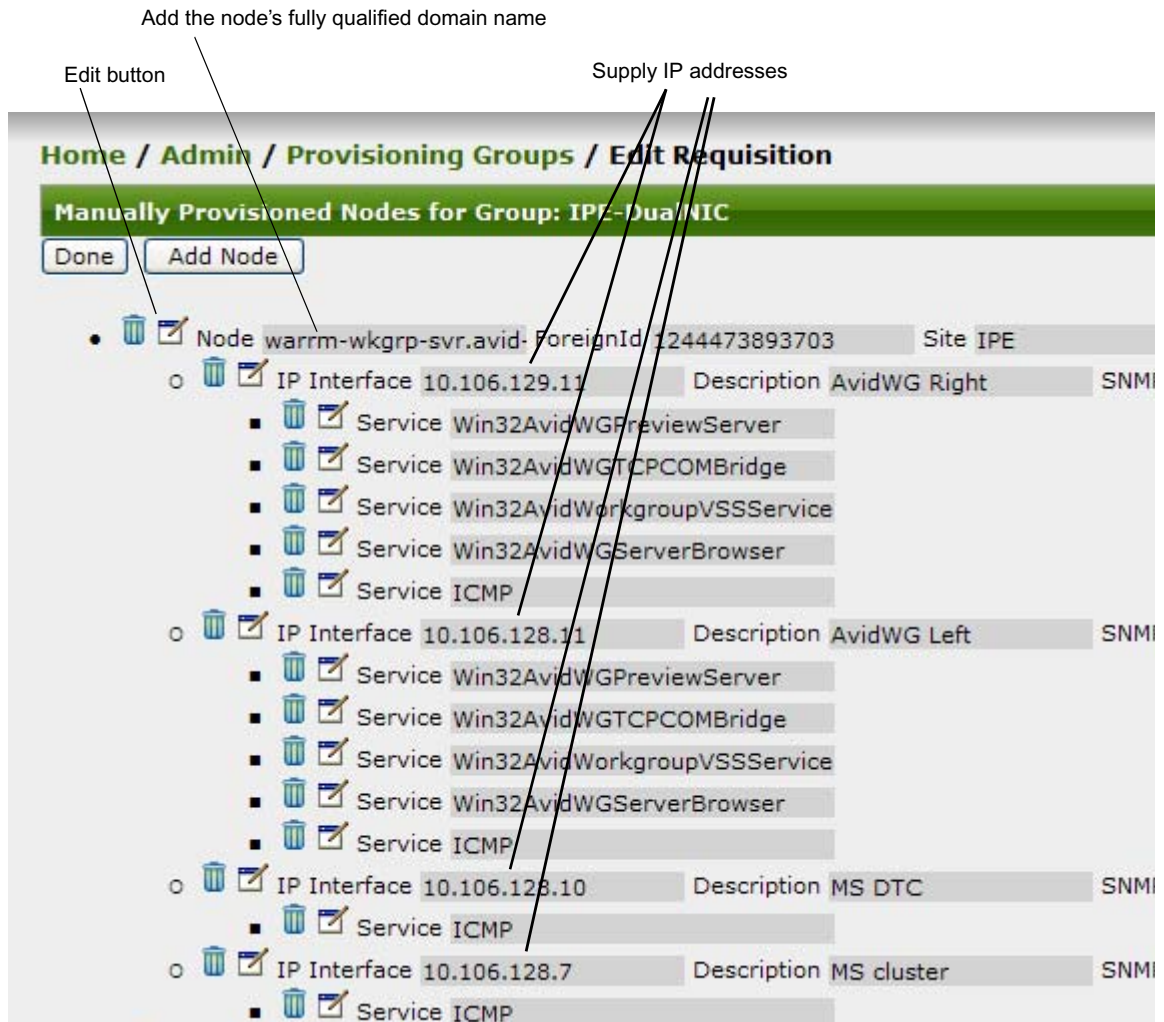
To edit the Provisioning Group values:

1. Click the Provisioning Group Edit button for the provisioning group you are going to edit (IPE-DualNIC or IPE-SingleNIC).

This example assumes that you have selected the dual connected template.

The system opens and displays the template.

The following illustration shows the virtual node portion of the template already configured. Notice that the virtual node runs the cluster services. This ensures that if the physical nodes fail over, the cluster services will still show as running.



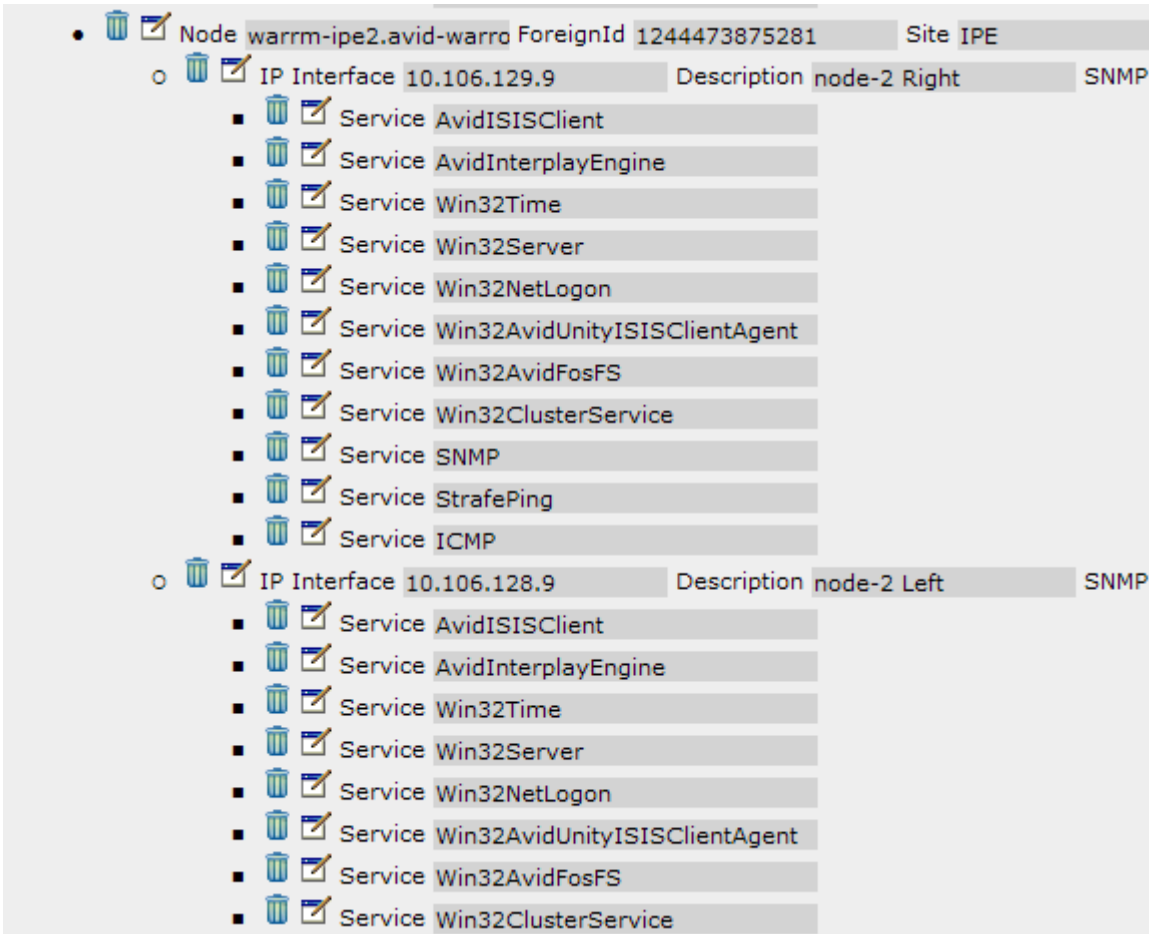
2. Click the Edit button for the node name and add the qualified domain name of the virtual Interplay engine. This is also referred to as the Interplay Server name. This is the name that clients use to connect to the Interplay Engine.
3. Click Save.
4. Click the Edit button for the first IP interface and add the IP address for the right side of the network. (The default description for this interface is AvidWG Right) Then click the Save button.

5 Working with Provisioning Groups

Rather than using the default descriptions of AvidWG Left and AvidWG Right, you can use any name that works for your site such as VLAN10 and VLAN20. The point is to be consistent on all the interfaces for this provisioning group.

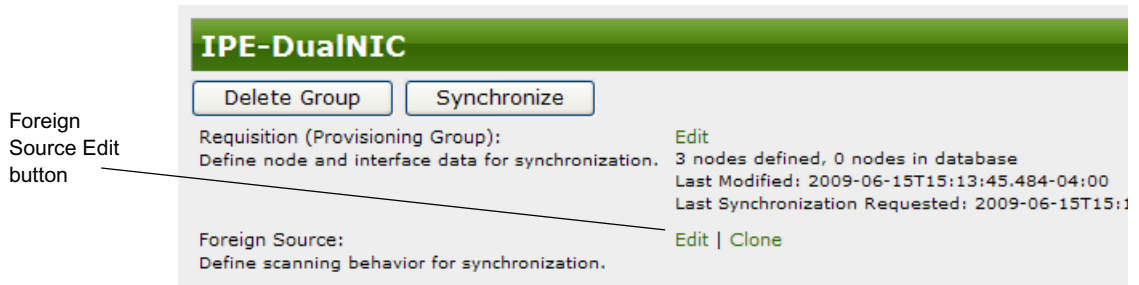
5. Add the IP addresses for the other interfaces on the virtual node, clicking Save each time.
6. Click the Done button to record your changes.
7. Perform the same steps for the two physical nodes and click Done to save your changes.

The following illustrations show the completed layout for the second physical node. Compare the fully qualified domain name and the IP addresses with the values in the table at the beginning of this section.



To delete the Foreign Source detectors:

1. Click the Foreign Source Edit button



The Foreign Source editing window opens.

2. Click each trash can icon and delete all of the detectors on the page.
3. Click Done.

To instruct OpenNMS to use the updated provisioning group file:

- Click the Synchronize button for the IPE-DualNIC provisioning group name.

OpenNMS imports the template, adds the nodes to OpenNMS, and displays the date of the import in the Last Synchronize Request and Last Changed columns.



It might take a few minutes for the node to appear in the Node List.

To verify that the cluster is configured:

1. Click Node List at the top of the OpenNMS window and look for the fully qualified domain name of the virtual node that you just added. In this case it is WARRM-WKGRP-SVR.avid-warroom.com.
2. Click the node name in the Node List.

The system displays the page for the virtual node. The following illustration shows the virtual node for this example.

5 Working with Provisioning Groups

[Home](#) / [Search](#) / [Node](#)
Node: warrm-wkgrp-svr.avid-warroom.com
Foreign Source: IPE-DualNIC

[View Events](#) [View Alarms](#) [View Outages](#) [Asset Info](#) [Site Status](#) [Resource Graphs](#) [Rescan](#) [Admin](#) [Schedule Outages](#)

SNMP Attributes		
Name	WARRM-IPE1	
Object ID	.1.3.6.1.4.1.311.1.1.3.1.2	
Location	Avid CS Hardware Lab	
Contact	Mike	
Description	Hardware: x86 Family 6 Model 15 Stepping 11 AT/AT COMPATIBLE - Software: Windows Version 5.2 (Build 3790 Multiprocessor Free)	

Availability		
Availability (last 24 hours)	100.000%	
10.106.128.7	Overall	100.000%
	ICMP	100.000%
10.106.128.10	Overall	100.000%
	ICMP	100.000%
10.106.128.11	Overall	100.000%
	ICMP	100.000%
	Win32AvidWGPreviewServer	100.000%
	Win32AvidWGServerBrowser	100.000%
	Win32AvidWGTCPCOMBridge	100.000%
	Win32AvidWorkgroupVSSService	100.000%
	Overall	100.000%
	ICMP	100.000%
	Win32AvidWGPreviewServer	100.000%

General (Status: Active)		
View Node IP Route Info		
View Node Link Detailed Info		

Surveillance Category Members		
Interplay Database Engines		
Warroom Lab		

Notification		
You: Outstanding: (Check)		
You: Acknowledged: (Check)		

Recent Events			
☐ 48355	8/24/11 13:06:17		No
☐ 397	8/23/11 13:06:16		No
☐ 395	8/23/11 13:06:15		W.
☐ 394	8/23/11 13:06:15		W.
☐ 393	8/23/11 13:06:15		W.
			More

Recent Outages		
There have been no outages on this		

3. Use the same technique to verify that the two physical nodes are added. You could also click the Search link and search for nodes running the AvidInterplayEngine service.

Interplay Engines and ISIS v2.3 and v2.4

ISIS v2.3 and v2.4 made a change to the name of the ISIS client service that runs on nodes such as the Interplay Engine. The following shows the difference between the names:

- ISIS v2.2 and earlier: AvidISISClient
- ISIS v2.3 and v2.4: AvidUnityISISClient

The default provisioning group files for Avid System Monitor v1.2.1 use the AvidISISClient name. If your site is running ISIS v2.3 or v2.4 you need to change the name of the ISIS client service in the provisioning group for the Interplay Engine.

The following illustration shows the ISIS service as it appears for ISIS v2.2 or earlier.

ISIS v2.2 or earlier

10.106.128.8	Overall	100.000%
	AvidISISClient	100.000%
	AvidInterplayEngine	100.000%
	ICMP	100.000%
	SNMP	100.000%
	StrafePing	100.000%
	Win32AvidFosFS	100.000%
	Win32AvidUnityISISClientAgent	100.000%
	Win32ClusterService	100.000%
	Win32NetLogon	100.000%
	Win32Server	100.000%

The following illustration shows the ISIS client service as it appears for ISIS v2.3 or v2.4.

ISIS v2.3 or later

10.105.228.11	Overall	100.000%
	AvidInterplayEngine	100.000%
	AvidUnityISISClient	100.000%
	ICMP	100.000%
	SNMP	100.000%
	StrafePing	100.000%
	Win32AvidFosFS	100.000%
	Win32AvidUnityISISClientAgent	100.000%
	Win32ClusterService	100.000%
	Win32NetLogon	100.000%
	Win32Server	100.000%



ISIS versions after v2.4 will return to the AvidISISClient value.

Replacing the Service Before You Configure the Interplay Engine Provisioning Group

If this is a new install and you have not configured the Interplay Engine provisioning group, you can edit the source .xml file for the provisioning group file that you will use.

To edit the Interplay Engine provisioning group file:

1. Navigate to the following directory on the Avid System Monitor server:
OpenNMS/etc/imports
2. Edit one of the following files depending on the type of Interplay Engine you have:
 - IPE-Standalone.xml (non-cluster Interplay Engine)
 - IPE-SingleNIC.xml (cluster, single connection to ISIS)
 - IPE-DualNIC.xml (cluster, dual connected to ISIS)
3. Replace the text “AvidISISClient” with “AvidUnityISISClient” and save the file. The following illustration shows the string that must be changed.

```
<node node-label="node2.FQDN"
  foreign-id="1244473875281" building="IPE">
  <interface ip-addr="1.1.1.2" descr="node-2" status="1" snmp-primar
    <monitored-service service-name="AvidISISClient"/>
    <monitored-service service-name="AvidInterplayEngine"/>
    <monitored-service service-name="Win32Time"/>
    <monitored-service service-name="Win32Server"/>
    <monitored-service service-name="Win32NetLogon"/>
    <monitored-service service-name="Win32AvidUnityISISClientAgent
    <monitored-service service-name="Win32AvidFosFS"/>
    <monitored-service service-name="Win32ClusterService"/>
    <monitored-service service-name="SNMP"/>
    <monitored-service service-name="StrafePing"/>
    <monitored-service service-name="ICMP"/>
  </interface>
</node>
```



Depending on the type of Interplay Engine, the text may appear several times in the file. Change all occurrences. Do not change the Win32AvidUnityISISClientAgent value.

4. Now when you edit the provisioning group in the OpenNMS user interface the name will appear correctly for ISIS v2.3 and v2.4.

Replacing the Service After You Configure the Provisioning Group

If you have already used a provisioning group to add the Interplay Engine to OpenNMS and are running ISIS v2.3 or v2.4, use the OpenNMS user interface to create a new service and then delete the old service.

To create a new AvidUnityISISClient service:

1. Verify that the AvidISISClient service is not being monitored. Open the node page for the Interplay Engine and check the service. If its not being monitored, OpenNMS displays “0%” in the Availability column and “Down” in the Recent Outages area as shown in the following illustration.

10.105.228.11	Overall	91.667%
	AvidISISClient	0.000%
	AvidInterplayEngine	100.000%
	ICMP	100.000%
	SNMP	100.000%
	StrafePing	100.000%
	Win32AvidFosFS	100.000%
	Win32AvidUnityISISClientAgent	100.000%
	Win32ClusterService	100.000%
	Win32NetLogon	100.000%
	Win32Server	100.000%
	Win32Time	100.000%

Recent Outages			
Interface	Service	Lost	Regained
10.105.228.11	AvidISISClient	11/14/11 17:47:22	DOWN

2. Select Admin > Manage Provisioning Groups and navigate to the provisioning group you want to modify. In this example, select IPE-SingleNIC provisioning group. Notice that the provisioning group in the example is already being used and is monitoring three nodes.

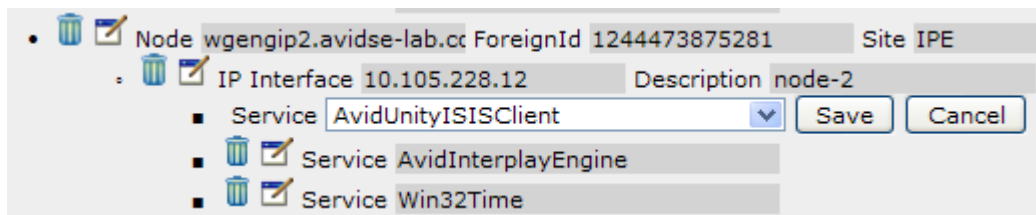
5 Working with Provisioning Groups

3. Click the Provisioning Group Edit button.
4. Scroll down to the first occurrence of AvidISISClient and click the corresponding Trash can button to delete the service.

 *Don't simply edit the existing service and change it to AvidUnityISISClient. Testing has shown that this may not succeed in removing the old service from the PostgreSQL database. It's better to delete the service and add a new one.*

5. Click the Add Service button on the far right side of the IP Interface line.

6. Select AvidUnityISISClient from the pop-up menu on the new service.



7. Click the Save Button.
8. Locate the remainder of the AvidISISClient service entries and delete and replace them with a new AvidUnityISISClient service. There are two for a single connected clustered Interplay Engine and four for a dual connected system.
9. Click Done at the top left of the window. OpenNMS displays the Provisioning Groups window.
10. Click Synchronize for the provisioning group you just edited.

The AvidUnityISISClient service appears in the availability list as shown in the following illustration. Notice that the old AvidISISClient service is still present and should be deleted.

Old service needs to be deleted	Overall	91.667%
	AvidISISClient	0.000%
New service is now added	AvidInterplayEngine	100.000%
	AvidUnityISISClient	100.000%
	ICMP	100.000%
	SNMP	100.000%
	StrafePing	100.000%
	Win32AvidFosFS	100.000%
	Win32AvidUnityISISClientAgent	100.000%

To remove a monitored service from OpenNMS:

1. Click the service name in the Availability column as shown in the previous illustration. In this example, click AvidISISClient.
- OpenNMS displays the page for that service.

5 Working with Provisioning Groups

Home / Search / Node / Interface / Service
AvidISISClient service on 10.105.228.11
[View Events](#) [Delete](#)

Delete button

General	
Node	wgengip1.avidse-lab.com
Interface	10.105.228.11
Polling Status	Managed

Recent Events	
☐ 206899	11/14/11 17:47:22
☐ 206887	11/14/11 17:47:12

Mo

Recent Outages	
Lost	
11/14/11 17:47:22	

Overall Availability	
0.000%	

Application Memberships (Edit)	
This service is not a member of any applications	

- Click Delete near the top left of the window and then click OK to confirm.

OpenNMS removes the service from the Availability column as shown in the following illustration.

Overall Availability	
100.000%	
Overall	Not Monitored
Overall	100.000%
AvidInterplayEngine	100.000%
AvidUnityISISClient	100.000%
ICMP	100.000%
SNMP	100.000%
StrafePing	100.000%
Win32AvidFosFS	100.000%
Win32AvidUnityISISClientAgent	100.000%
Win32ClusterService	100.000%
Win32NetLogon	100.000%
Win32Server	100.000%
Win32Time	100.000%

You: Outstanding: (Check)
 You: Acknowledged: (Check)

Recent Events			
☐ 252550	11/15/11 21:53:14	Warning	The AvidISISClient s 10.105.228.11.
☐ 252549	11/15/11 21:53:14	Warning	The AvidISISClient s 10.105.228.11.
☐ 252548	11/15/11 21:53:14	Warning	The AvidISISClient s scheduled for deletio
☐ 243270	11/15/11 16:21:51	Normal	The Node with Id: 5; ForeignId:124447358
☐ 243269	11/15/11 16:21:51	Warning	SNMP information on collection purposes.

More...

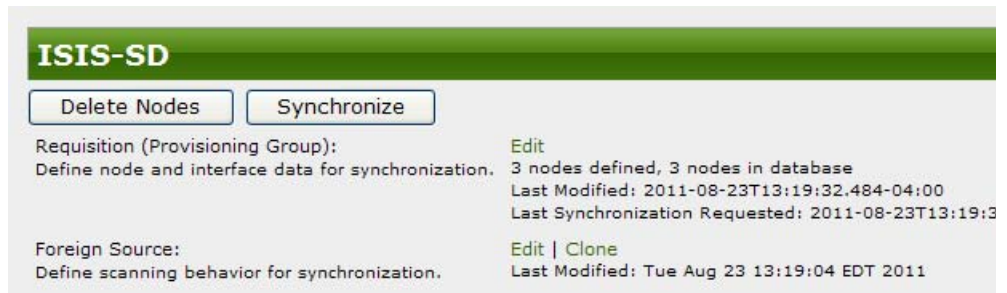
Recent Outages	
There have been no outages on this node in the last 24 hours.	

Using Provisioning Groups to Configure an ISIS 7000 System Director

To configure the ISIS System Director template into OpenNMS:

1. Launch the OpenNMS interface and click the Admin link.
2. In the Nodes area, select Manage Provisioning Groups.

The following illustration shows the Provisioning Group page with the ISIS-SD entry after the template has been edited and synchronized. Notice that it shows 3/3 meaning that there are 3 nodes in the group and 3 nodes are now configured in the database.



3. Click the ISIS-SD group name to open the Provisioning Groups page.
4. Edit the Provisioning Group as described for the Interplay Engine.
5. Click Done to save your changes and then click Synchronize for the ISIS-SD Group Name.

The system imports the template and displays the date of the import in the Last Import Request and Last Changed columns on the right side of the window.

The following illustration shows the virtual ISIS node and one physical node completed. Compare the values to the table at the beginning of the section.

Home / Admin / Provisioning Groups / Edit Requisition

Manually Provisioned Nodes for Group: ISIS-SD-WR

- Node **warm-isis.avid-warroc** ForeignId **1244483422718** Site **ISIS**
 - IP Interface **10.106.129.4** Description **Right** SNMP
 - Service **AvidISISSystemDirector**
 - Service **AvidISISSnmp**
 - Service **SNMP**
 - Service **ICMP**
 - IP Interface **10.106.128.4** Description **Left** SNMP
 - Service **AvidISISSystemDirector**
 - Service **AvidISISSnmp**
 - Service **SNMP**
 - Service **ICMP**
- Node **warm-sd2.avid-warroc** ForeignId **1244482712531** Site **ISIS**
 - IP Interface **10.106.129.6** Description **Right** SNMP
 - Service **Win32AvidUnityISISSystemDirect**
 - Service **Win32AvidUnityISISAdminServer**
 - Service **Win32Time**
 - Service **Win32Server**
 - Service **SNMP**
 - Service **StrafePing**
 - Service **ICMP**



A total of 6 IP addresses must be added for an ISIS cluster system.

Configuring an Interplay Stream Server

There are two template files to define an Interplay Stream Server. The following templates are supplied as part of the custom Avid configuration files.

- IPSS-dualNIC
- IPSS-singleNIC

The two templates are for a dual connected or single connected Stream Servers. Use these templates similarly to how you would configure an Interplay Engine standalone system. Also see [“Changes for the Stream Server” on page 152](#).

Defining Nodes with Basic Up/Down Status

This section describes how to use the NodeUpDownStatus provisioning group template to add nodes to OpenNMS. You can use this template to add many different nodes to OpenNMS. For an example of the nodes that you can add with this template, see the table in [“Methods for Discovering Systems to be Monitored” on page 110](#).



You can create different templates to monitor the Up/Down status of different types of nodes. This makes it easier to modify the template and add new nodes. For example, you could create one specifically for ingest/payout devices. See [“Creating New Provisioning Groups” on page 106](#).

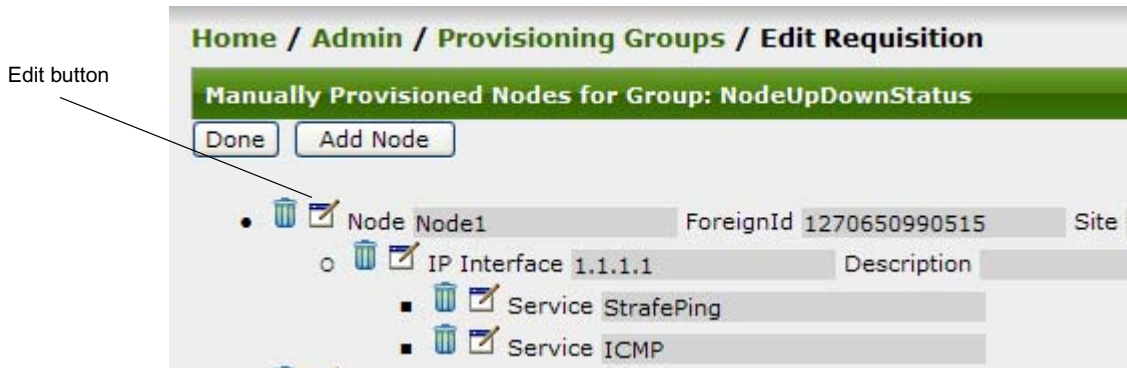
To use the NodeUpDownStatus template:

1. Click the Admin link in OpenNMS.
2. Under the Nodes section, click Manage Provisioning Groups.
The Provisioning Groups window opens.
3. Locate the NodeUpDownStatus section.

The screenshot shows the 'NodeUpDownStatus' provisioning group template. It has a green header with the title. Below the header are two buttons: 'Delete Group' and 'Synchronize'. The main content area is divided into two columns. The left column contains the text 'Requisition (Provisioning Group):' followed by 'Define node and interface data for synchronization.' and 'Foreign Source:' followed by 'Define scanning behavior for synchronization.' The right column contains the text 'Edit' followed by '5 nodes defined, 0 nodes in database', 'Last Modified: 2010-04-07T10:36:51.078-04:00', 'Last Synchronization Requested: Never', and 'Edit | Clone'.

4. Click the Provisioning Groups Edit button. OpenNMS opens the template for editing.
5. Click the Edit button for the first available node. By default, available nodes are named Node1, Node2, etc.

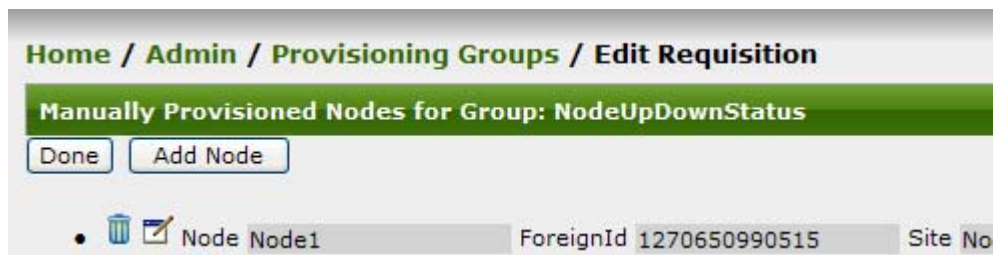
5 Working with Provisioning Groups



6. Enter the fully qualified domain name of the node and click Save at the end of the line.
7. Click the Edit button for the IP Interface.
8. Enter the IP address for this node and click Save.
9. Repeat the process for other nodes that you want to add.
10. When you are finished adding nodes, click Done.

To add additional nodes to the template.

1. Click the Add Node button.



2. Type in the fully qualified domain name and click Save.

Node name

Manually Provisioned Nodes for Group: NodeUpDownStatus

Done Add Node

- Node New Node ForeignId 1314297567180 Site
- Node Node1 ForeignId 1270650990515
 - IP Interface 1.1.1.1 Description
 - Service StrafePing
 - Service ICMP

3. Click Add Interface near the end of the line.

Site NodeUpDownStatus Save Cancel

Site NodeUpDownStatus [Add Interface] [Add Node Category] [Add Node Asset]

SNMP Primary P Add Service

4. Type in the IP address of the node and click Save.
5. Click Add Service.
6. Select ICMP and click Save.
7. Click Add Service, select Strafeping and click Save.
8. Click Done.

To instruct OpenNMS to use the updated provisioning group file:

- Click the Synchronize button for the NodeUpDownStatus provisioning group.
OpenNMS imports the template, adds the nodes to OpenNMS, and displays the date of the import in the Last Synchronize Request and Last Changed columns.



It might take a few minutes for the node to appear in the Node List.

Creating New Provisioning Groups

You can create custom provisioning group templates with specific names to make them easier to identify. For example, the following OpenNMS system monitors Interplay Engines from several different labs and there is a separate Provisioning group template for each one.

The screenshot displays the OpenNMS Provisioning Groups management interface. It features four distinct provisioning group templates, each with a green header bar and a light gray content area. Each template includes buttons for 'Delete Nodes' and 'Synchronize', and details for 'Requisition (Provisioning Group)' and 'Foreign Source'.

IPE-SingleNIC

Delete Nodes Synchronize

Requisition (Provisioning Group):
Define node and interface data for synchronization.

Foreign Source:
Define scanning behavior for synchronization.

Edit
3 nodes defined, 3 nodes in database
Last Modified: 2011-08-23T13:07:35.093-04:00
Last Synchronization Requested: 2011-08-23T13:07:35.281-04:00

Edit | Clone
Last Modified: Tue Aug 23 15:06:46 EDT 2011

IPE-SingleNIC-A51

Delete Nodes Synchronize

Requisition (Provisioning Group):
Define node and interface data for synchronization.

Foreign Source:
Define scanning behavior for synchronization.

Edit
3 nodes defined, 3 nodes in database
Last Modified: 2011-08-23T16:32:39.765-04:00
Last Synchronization Requested: 2011-08-23T16:32:39.937-04:00

Edit | Clone
Last Modified: Tue Aug 23 13:12:12 EDT 2011

IPE-StandAlone-B3

Delete Nodes Synchronize

Requisition (Provisioning Group):
Define node and interface data for synchronization.

Foreign Source:
Define scanning behavior for synchronization.

Edit
1 nodes defined, 1 nodes in database
Last Modified: 2011-08-23T16:00:16.390-04:00
Last Synchronization Requested: 2011-08-23T16:00:16.828-04:00

Edit | Clone
Last Modified: Tue Aug 23 15:49:21 EDT 2011

IPE-StandAlone-SC

Delete Nodes Synchronize

To create a new provisioning group:

1. Select Admin > Manage Provisioning Groups.
2. At the top of the Provisioning Groups page, type in the name for the provisioning group template and click Add New Group as shown in the following illustration.

Home / Admin / Provisioning Groups

New group name — IPE-DocLab Add New Group Edit Default Foreign Source Re:

IPE-DualNIC

Delete Nodes Synchronize

Requisition (Provisioning Group): Define node and interface data for synchronization. Edit
3 nodes defined, 3 nodes in database
Last Modified: 2011-08-23T13:06:15.125-04:00
Last Synchronization Requested: 2011-08-23T13:

Foreign Source: Define scanning behavior for synchronization. Edit | Clone
Last Modified: Tue Aug 23 13:12:03 EDT 2011



The system creates a file with the same name in `\OpenNMS\etc\imports`. Do not use blank spaces or special characters in the name.

The following illustration shows the new provisioning group.

Home / Admin / Provisioning Groups

Add New Group Edit Default Foreign Source Reset Default Foreign So

IPE-DocLab

Delete Group Synchronize

Requisition (Provisioning Group): Define node and interface data for synchronization. Edit
0 nodes defined, 0 nodes in database
Last Modified: 2011-08-26T11:27:16.313-04:00
Last Synchronization Requested: Never

Foreign Source: Define scanning behavior for synchronization. Edit | Clone

3. Edit the new provisioning group and add nodes and services as described in “Defining Nodes with Basic Up/Down Status” on page 103.



Do not create a new provision group by copying and renaming one of the templates in `\etc\imports`. You must use the OpenNMS interface to create a new template.

For additional information on provisioning groups see the OpenNMS Provisioning white paper on the OpenNMS web site:

http://www.opennms.org/wiki/White_Papers

6

Configuring Discovery and the Dashboard

This chapter describes how to configure Avid Monitor System to discovery nodes in your environment and to present node information in a useful way on the dashboard.

- [Methods for Discovering Systems to be Monitored](#)
- [Deleting the Default Discovery Range](#)
- [Configuring Discovery Using Add Interface](#)
- [Configuring the Dashboard](#)
- [Naming the Discovered Nodes](#)

Methods for Discovering Systems to be Monitored

Systems that are being monitored are referred to as nodes. You can use the OpenNMS interface to add nodes. There are several methods for adding nodes, referred to as the Discovery method in the following table:

System	Software to install	Configure SNMP	Method used to add to OpenNMS
Interplay Engine single system	Interplay SNMP agent	Yes	Provisioning group IPE-Standalone template
Avid Interplay Engine cluster system	Interplay SNMP agent	Yes	Provisioning group IE DualNIC or IE SingleNIC template
Interplay Stream Server	Interplay SNMP agent	Yes	Provisioning group IPSS DualNIC or IPSS SingleNIC template
Avid ISIS 7000 System Director	ISIS SNMP Agent Enable SNMP Trap Events	Yes	Provisioning group ISIS-SD template
Avid ISIS 5000 System Director	Enable SNMP Trap Events	Yes	Add Interface
Network switches (Foundry, Cisco, and Force10)	NA	Yes	Add Interface
Media Indexer and AirSpeed Multi Stream v1.8.1 or higher	Monitoring Gateway	Yes	Add Interface
Interplay Capture	Monitoring Gateway	No	Add Interface
System running Avid Service Framework Lookup Service	Monitoring Gateway	Yes	Add Interface
System running Active Directory and DNS	NA	Yes	Add Interface
Other Interplay servers: Interplay Transfer, Media Services, etc.	NA	No	Provisioning group: NodeUpDownStatus
Other Intel servers you want to monitor	NA	No	Provisioning group: NodeUpDownStatus
Avid editing systems	NA	No	Not monitored

Provisioning Groups versus Add Interface

When you configure systems for discovery, you use Add Interface for some and provisioning groups for others. The main differences between the two are as follows:

- The Add Interface command allows OpenNMS to discover all of the services running on a system. For an example of how this form of discovery works, see [“An Example Monitoring Workflow for Automatic Discovery” on page 19](#). Every 24 hours OpenNMS reruns the discovery process on the node. If any additional services have been added they will be identified and added to the database.
- Provisioning groups allow you to specify the services that you want to monitor. This is important for cluster systems because it allows you to define a set of services that run on the Virtual Interplay Engine or Virtual ISIS Engine. Provisioning groups also allow you to focus on specific services and avoid additional events and alarms that may represent false positives or false negative values. See [“Working with Provisioning Groups” on page 83](#).

OpenNMS also allows you to configure nodes using an IP address range via the Admin > Configure Discovery window. This method is not supported for this release in order to focus only on the nodes and services that have been qualified.

Configuring Discovery Using Add Interface

In Avid System Monitor, systems that are being monitored are referred to as nodes. You can use the OpenNMS interface to add nodes.

This section describes how to use the Add Interface command to add nodes. When you use this method, OpenNMS automatically discovers and examines the node you specify. For information on the discovery process, see [“An Example Monitoring Workflow for Automatic Discovery” on page 19](#).



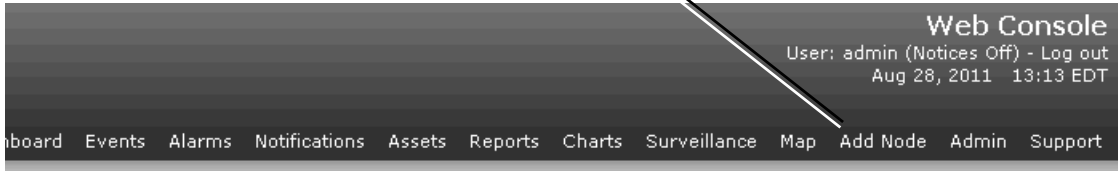
Do not use the Add Interface command to add Interplay Engine, Stream Server, or ISIS 7000 systems. See [“Methods for Discovering Systems to be Monitored” on page 110](#).



Do not use the Add Node menu item on the top bar of the OpenNMS interface. Use Admin > Add Interface.

6 Configuring Discovery and the Dashboard

Do not use Add Node.
Use Admin > Add Interface instead



Before you begin, determine the IP addresses of the following systems:

- Media Indexers that are monitoring shared storage
- The system running the Avid Service Framework Lookup Service
- Interplay Capture systems
- Network Switches



For information on using the Add Interface command to add a network switch, see “Using Add Interface to Add a Network Switch to OpenNMS” on page 79.

Using the Add Interface Command to Add Nodes

This section describes how to use the Add Interface command to define nodes for Discovery. Discovery is useful for systems that are running the Avid Monitoring gateway. OpenNMS uses the Avid Monitoring Gateway to discover Avid-specific services on those nodes.

To add nodes to the Avid System Monitor configuration:

1. Click the Admin link and select Add Interface under the Nodes section.
2. Type in the IP address of the system you want to monitor and click Add.



If the node has more than one NIC, you only need to add one IP address. The additional NICs will be automatically identified during the discovery process. For additional information, see “An Example Monitoring Workflow for Automatic Discovery” on page 19.

3. To add additional interfaces, click the Browser Back button to return to the Enter IP Address page and click Add.

4. Click Node List to view the new nodes.

Note that the Discovery process may take a several minutes depending on the number of systems you add.

Deleting the Default Discovery Range

During the OpenNMS installation, the system prompts you for a default IP address range. If you accepted the default, use this procedure to delete the node range.

To delete the default IP address range for Discovery:

1. Click the Admin link and select Configure Discovery under the Operations section.
2. Locate the Include Ranges section as shown in the following illustration.

Include Ranges

Add New

Begin Address	End Address	Timeout (ms.)
192.168.0.1	192.168.0.254	200

Exclude Ranges

Add New

No exclude range defined.

Save and Restart Discovery

The default range is 192.168.0.1 through 192.168.0.254.

3. Click the Delete button on the far right side of the range.
4. Click Save and Restart Discovery at the bottom of the page.

Configuring the Dashboard

This section describes how to configure the OpenNMS dashboard and surveillance categories.

 After you copy the Avid specific config files onto the OpenNMS server, clicking Surveillance at the top of the OpenNMS window returns an error until you configure the Dashboard. This is because the Avid-specific config files do not match the default OpenNMS Surveillance categories in the user interface.

Determine the Category Names for the Site

The following illustration shows an example of a dashboard configuration. The types of nodes are identified by the rows. The location or use of the nodes is identified by the columns on the right side.

Surveillance View: default		
Show all nodes	Production	Standby Systems
ISIS System Directors	0 of 1	0 of 0
Ingest and Payout	0 of 0	0 of 0
Interplay Database Engines	0 of 1	0 of 0
Interplay Services	0 of 1	0 of 0
LAN Switches	0 of 0	0 of 0
Network Services - AD, DNS, DHCP	0 of 0	0 of 0

Avid recommends that you use the same names of the rows for consistency and customize the names of the columns for your site. The above illustration uses Production, Standby Systems, and Development Systems to categories different nodes. At a large site you may have nodes in different Interplay environments or workgroups. In that case you could name the three columns Workgroup 1, Workgroup 2, and Workgroup 3 or use the actual names of your workgroups.

Delete the Default Surveillance Categories and Add New Ones

Surveillance categories define the Dashboard and front page display. You must delete the default list of surveillance categories in the OpenNMS interface and add the Avid-specific entries.

Categories are defined as rows and columns. You can add nodes to more than one category. For example, in the previous illustration you add nodes to the Interplay Services category and then you decide whether the nodes belong in the Production, Standby Systems, or Development categories.

To view and edit the dashboard settings in the surveillance-views.xml file:

1. Open the following file with an application such as Notepad:
Program Files\OpenNMS\etc\surveillance-views.xml
2. Notice the lines that designate rows and columns.
3. (Option) Change the names of the columns to match the columns you want to use in your dashboard. For example, change the three column names to the following:
 - Production

- Standby Systems
- Development Systems

You can use any names that are appropriate for your site or accept the three default values.

4. Save the file and keep it open so you can add the same values to the OpenNMS Surveillance Categories interface.

To delete the default surveillance categories and add new ones:

1. Open the surveillance-views.xml file as described above.
2. On the Avid System Monitor Home page, click Admin.
3. Under the Nodes area, click Manage Surveillance Categories. The following illustration shows the default list of Surveillance categories.

Home / Admin / Categories		
Surveillance Categories		
Delete	Edit	Category
		Development
		Production
		Routers
		Servers
		Switches
		Test
		Add New Category

4. Click the Trash can for each category to delete all of the default categories.
5. Type the name of a new category (for example, Ingest and Playout) in the text box next to the Add New Category button. The name must match one of the names in the surveillance-views.xml file exactly (including upper and lower case).



The best way to ensure that you match the names is to open the surveillance-views.xml file in an application such as Notepad and then copy and paste the text into the OpenNMS interfaces.

6. Click Add New Category. The new category appears in the list. The following illustration shows all the new categories added. In this example, the columns are named Workgroup 1, Workgroup 2, and Workgroup 3).

6 Configuring Discovery and the Dashboard

Surveillance Categories		
Delete	Edit	Category
		ISIS System Directors
		Ingest and Playout
		Interplay Database Engines
		Interplay Services
		LAN Switches
		Network Services - AD, DNS, DHCP
		Workgroup 1
		Workgroup 2
		Workgroup 3
		Add New Category

7. Repeat the process for the remainder of the categories including the column categories. The following table shows the list of suggested values.

Surveillance Categories	Nodes	Row/Column
ISIS System Directors	System Directors	Row
Ingest and Playout	AirSpeed Multi Stream, AirSpeed Classic, Capture, and other ingest and playout devices	Row
Interplay Database Engines	Interplay Engines	Row
Interplay Services	Interplay Engines, Interplay Media Indexer servers, Interplay Media Services servers and providers, Interplay Transfer	Row
LAN Switches	Switches For example, Cisco and Foundry switches	Row
Network Services - AD, DNS, DHCP	Systems running AD, DNS, and DHCP	Row
For the three column values, either enter the default names (Workgroup, Test Lab, and Future Use) or supply your own names.	Groups nodes in columns	column

The names must match the Surveillance Category names in the table exactly (including upper and lower case). As mentioned earlier, you can copy and paste the names from the `surveillance-views.xml` file to make sure the names match.

Trouble Shooting

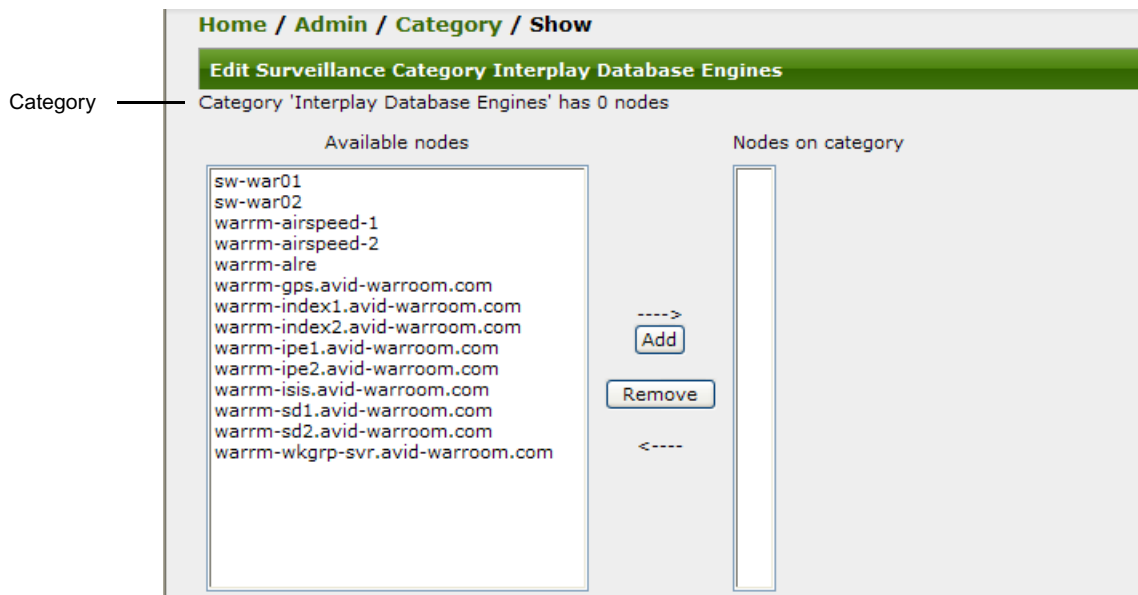
If OpenNMS won't start after you edit the `surveillance-views.xml` file, check the file to make sure that you did not introduce any .xml errors. Even deleting one quotation mark by mistake can make the file invalid. If necessary, you can copy a new version of the file from the `opennms_config` folder on the installer DVD.

Adding Nodes to Surveillance Categories

This section describes how to add nodes to Surveillance categories so they can be grouped by function on the dashboard. Perform this procedure after you have added nodes to your OpenNMS interface and they are appearing in the node list.

To add nodes to surveillance categories:

1. Click the OpenNMS logo to return to the Home page.
2. Click the Admin link and in the Nodes area, click Manage Surveillance Categories.
3. Click the Edit button for the category you want to add nodes to. The Edit Surveillance Category window opens. The following illustration shows the window for the Interplay Database Engines category.



6 Configuring Discovery and the Dashboard



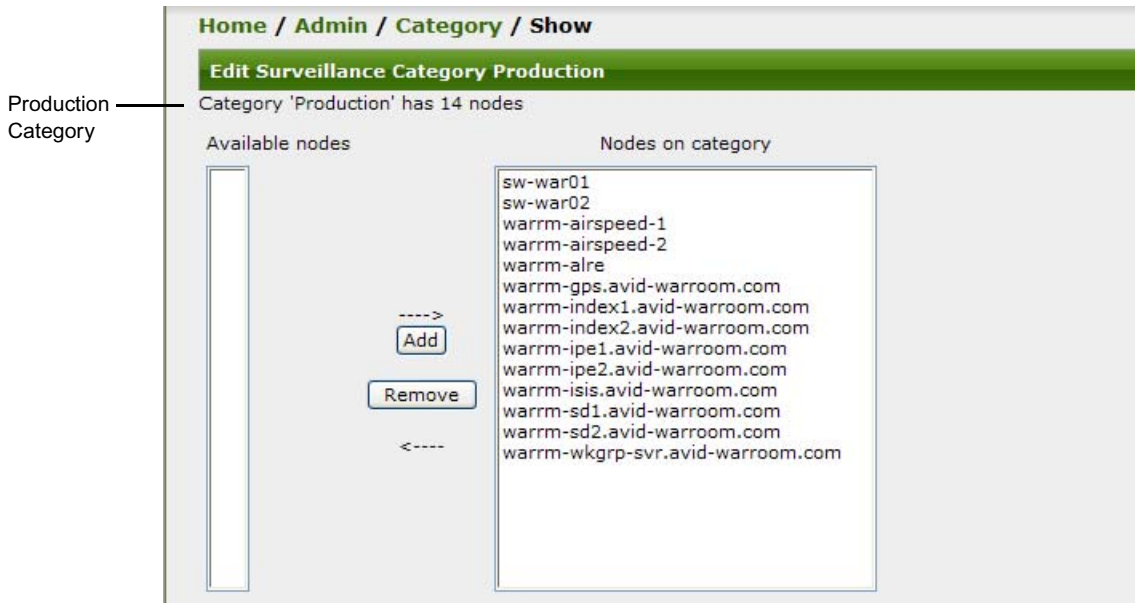
In this example, the default column category “Workgroup” has been renamed to Production.

4. Click the nodes that belong in the category and click the Add button. The nodes are added to the category.



You can use Shift-click or CTRL-click to select nodes from the list.

5. Click Category on the path at the top of the page to return to the Manage Surveillance Categories page.
6. Repeat the process for the other categories.
7. Also add the nodes to the column categories you defined. The nodes must belong to at least one row and one category in order to display on the dashboard. In this example, all of the servers are Production servers so they are all added to the Production category that we added as an example column.



8. Restart OpenNMS. See [“Restarting or Stopping OpenNMS”](#) on page 51.

To view the dashboard:

1. Click the OpenNMS logo to return to the Home page.
2. Click the Dashboard link.
3. Click one of the categories on the left. The system shows the nodes in that category at the bottom of the page. The following illustration shows the finished categories.

Node List Search Outages Path Outages Dashboard Events Alarms Notifications A

Home

Surveillance View: default

Show all nodes	Production	Standby System
ISIS System Directors	0 of 1	0 of 0
Ingest and Playout	0 of 0	0 of 0
Interplay Database Engines	0 of 1	0 of 0
Interplay Services	0 of 1	0 of 0
LAN Switches	0 of 0	0 of 0
Network Services - AD, DNS, DHCP	0 of 0	0 of 0

Alarms << 1 to 5 of 5

 Nodes do not appear in the Dashboard until they are in both a row and a column category.

Naming the Discovered Nodes

Naming nodes is optional. Naming the nodes makes it easier for other people in your organization to identify the nodes in the Avid System Monitor interface. Click the Node List to see the nodes that Avid System Monitor has discovered. Nodes that are registered in DNS have their fully qualified domain names, such as docwg.global.avidww.com.

To name a node:

1. Click the Node List and click the node that you want to name. In this example we will name the Interplay Engine.
2. The system displays the information for the node.

Node name Admin link

Home / Search / Node
Node: b3scaleinterpla.global.avidww.com
View Events View Alarms Asset Info HTTP Resource Graphs Rescan Admin Update St

General (Status: Active)
View Node Link Detailed Info

Notification
You: Outstanding: (You: Acknowledged

3. Click the Admin link. The Node Management window opens.

6 Configuring Discovery and the Dashboard

Home / Admin / Node Management
Node: b3scaleinterpla.global.avidww.com

Admin Options	Option Description
Change Node Label	Change Node Label select the node name.
Manage and Unmanage Interfaces and Services	When OpenNMS was first installed, the network grows and changes within those ranges, in your OpenNMS configuration...
Configure SNMP Data Collection per Interface	
Delete Node	
Configure Path Outage	

4. Under Admin Options, click Change Node Label.
5. Click User Defined and type in a descriptive name for the node. In this case we leave the domain name and type in Interplay Engine.

Home / Admin / Change Node Label

Current Label
b3scaleinterpla.global.avidww.com (DNS Hostname)

Choose a New Label
You can either specify a name or allow the system to automatically select the name.

User Defined
☒ Interplay Engine b3scaleinterpla.glc

Automatic
☐ b3scaleinterpla.global.avidww.com (DNS Hostname)

6. Click Change Label.



You must click Change Label for the change to take effect.

7. Return to the Node List and repeat the naming process for the rest of the nodes.

7 Working With Notifications and Maps

This chapter describes the following topics:

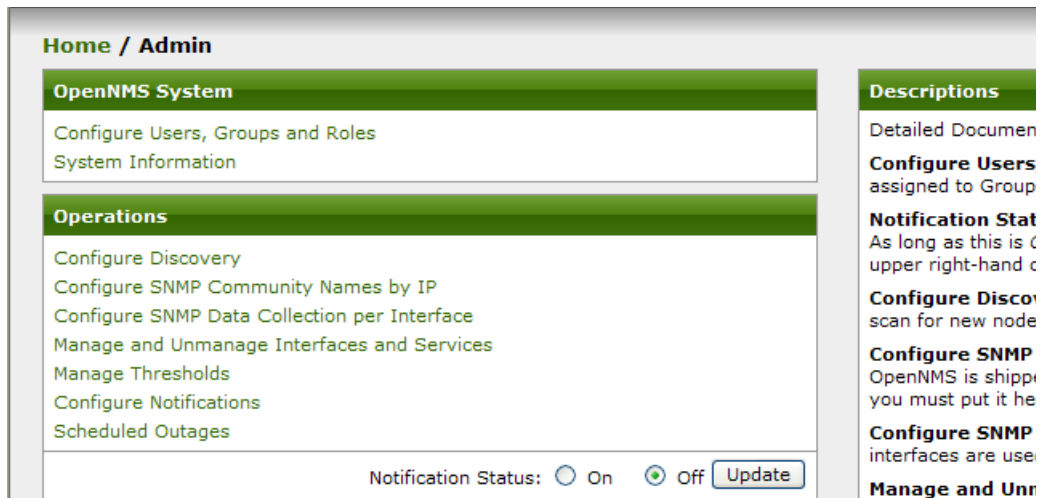
- [Working with Email Notifications](#)
- [Sending Notifications to An External Monitoring System](#)
- [Working with Maps](#)

Working with Email Notifications

This section describes how to configure email notifications.

Turning Notifications On and Off Globally

You can turn the notification feature on and off from the Admin panel. The following illustration shows the On and Off buttons.



To turn notifications on or off:

- Click Admin and under Operations click On or Off and then click Update.

Preparing the OpenNMS Server for Email Notification

In order to send email notifications, you must define the following:

- The sender account for email notifications
- The local mail server (SMTP host)

To define the sender account and SMTP host for Avid System Monitor:

1. Navigate to the following directory:
Program Files/OpenNMS/etc
2. Open the following file in Wordpad:
javamail-configuration.properties
3. Locate the following text near the top of the file:

```
#  
# This property defines the system sender account.  
#
```



Defining the sender account is not required to turn on email notification but it makes it easy to identify the incoming emails.

4. The default file contains generic values for the email sender. Uncomment the lines and type in an appropriate name that will identify that the email has come from the Avid System Monitor. The email must include the domain that contains the Avid System Monitor.

For example, the following line identifies the lab where the Avid System Monitor is running:

```
#  
# This property defines the system sender account.  
#  
# The default setting is root@[127.0.0.1]  
org.opennms.core.utils.fromAddress=warroom-lab@avid-warroom.com
```

Replace the “warroom...” string with an appropriate email address so that you can identify the sending account.

5. Locate the following text near the top of the file:

```
#  
# These properties define the SMTP Host.  
#
```

6. The default file contains generic values for the SMTP host. Supply your site-specific values for your SMTP host.

The following shows an example:

```
#
# These properties define the SMTP Host.
#
org.opennms.core.utils.mailHost=tewk-mailgw.global.avidww.com
org.opennms.core.utils.mailer=smtplib
```

7. Save and close the file.
8. Restart OpenNMS as follows:
 - a. Open the Windows Service Manager and locate the Avid Monitoring System service.
 - b. Restart the Avid Monitoring System service. See [“Restarting or Stopping OpenNMS” on page 51](#).

Assigning the Admin Email Account

You set up OpenNMS to route notifications to a path. In OpenNMS terms, a path can consist of one or more of the following:

- User
- Group
- Role
- Specific email address

You can define users, groups, and roles in the Admin area.

In this example we will specify the Admin email account for the site. Because all of the default notifications are defined to go to the Admin account, this is the easiest way to test the OpenNMS email notification.

To change or add an email to the Admin email account:

1. Click Admin along the top of the OpenNMS interface.
The Admin page opens.
2. Under the Operations section, click On for Notification Status and then click Update.

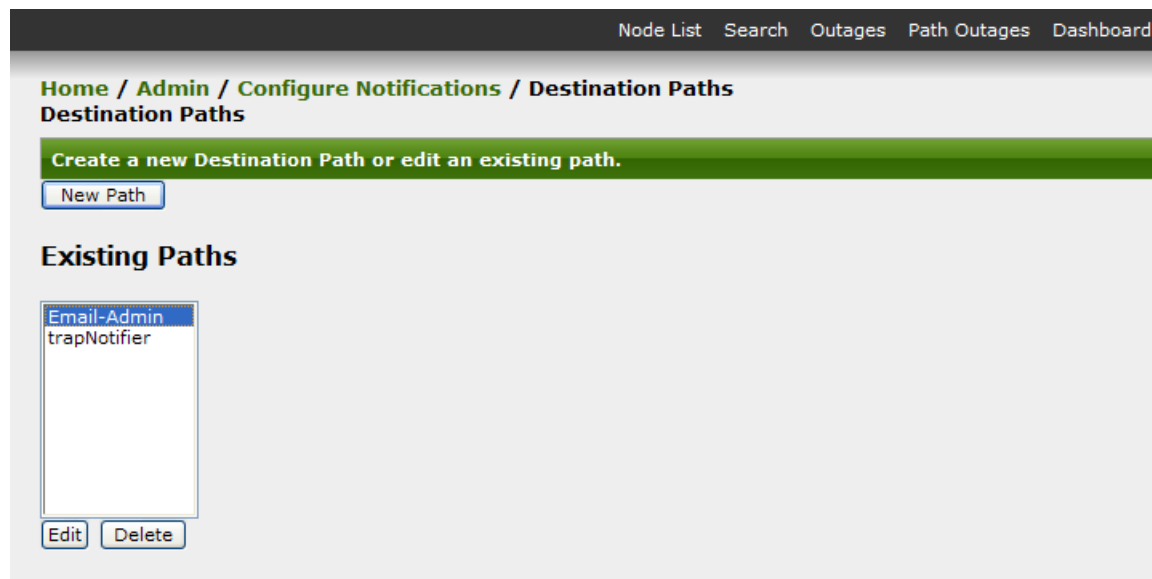


This is an important step. Notifications won't be sent until this button is On.

3. Click Configure Notifications in the Operations area.
The Configure Notifications page opens.
4. Click Configure Destination Paths

7 Working With Notifications and Maps

The Destination paths window opens.



5. Click Email-Admin and then click Edit.

The systems displays the email accounts assigned to the Email-Admin path.



The trapNotifier account is reserved for future use.

6. Select Admin and then click Edit in the window on the right.

The Choose Targets window opens.

Notification Paths / Choose Targets

Selected Groups:	Send to Selected Roles:	Send to Email Addresses:
Each group that needs to receive each user in the group will receive the notice.	Highlight each role that needs to receive the notice. The users scheduled for the time that the notification comes in will receive the notice.	Add any email addresses you want the notice to be sent to.
		Add Address email-name@domain-name.com Remove Address

- Remove the default email account and add the email accounts of the users that you want to be designated to receive admin email.



Depending on your browser you may have enable script windows or pop-ups to access the Add Address dialog box.

- Click the Next button and choose the delay before sending an email to this user.
- Click Next.



Other notification types such as javaPagerEmail have not been qualified for this release.

- Click Next again and click Finish.

Turning on Notifications and Specifying a Target Email Address

You can turn notifications on for particular events. Besides turning on the notification you must also edit the notification to specify the target email address.



Depending on how many times an event occurs, the system can potentially send many emails out in a very short period of time. Experiment with email notifications before you put them into use at your site.

To turn on a specific notification:

1. Click Admin > Configure Notifications.
2. Click Configure Event Notifications.

The Event Notifications window opens.

Actions			Notification
Edit	Delete	☒ Off ☐ On	AIMI Handle Count Too High
Edit	Delete	☒ Off ☐ On	Avid Capture Service Redundancy Weight Too Low
Edit	Delete	☒ Off ☐ On	Avid Clock Verification is Unresponsive

3. Scroll down the list and select the event that you want to turn notifications on for. In this example, select ISIS Error. This will turn on notifications for errors generated by the ISIS System Director.
4. Click the On button.
5. Click the Edit button associated with the notification.

The system displays a series of windows that show the details of the notification.

- Click Next and Skip Validation Results to step through these windows until you come to the Choose Path window.

Home / Admin / Configure Notifications / Choose Path
Editing notice: ISIS Error

Choose the destination path and enter the information to send via the notification

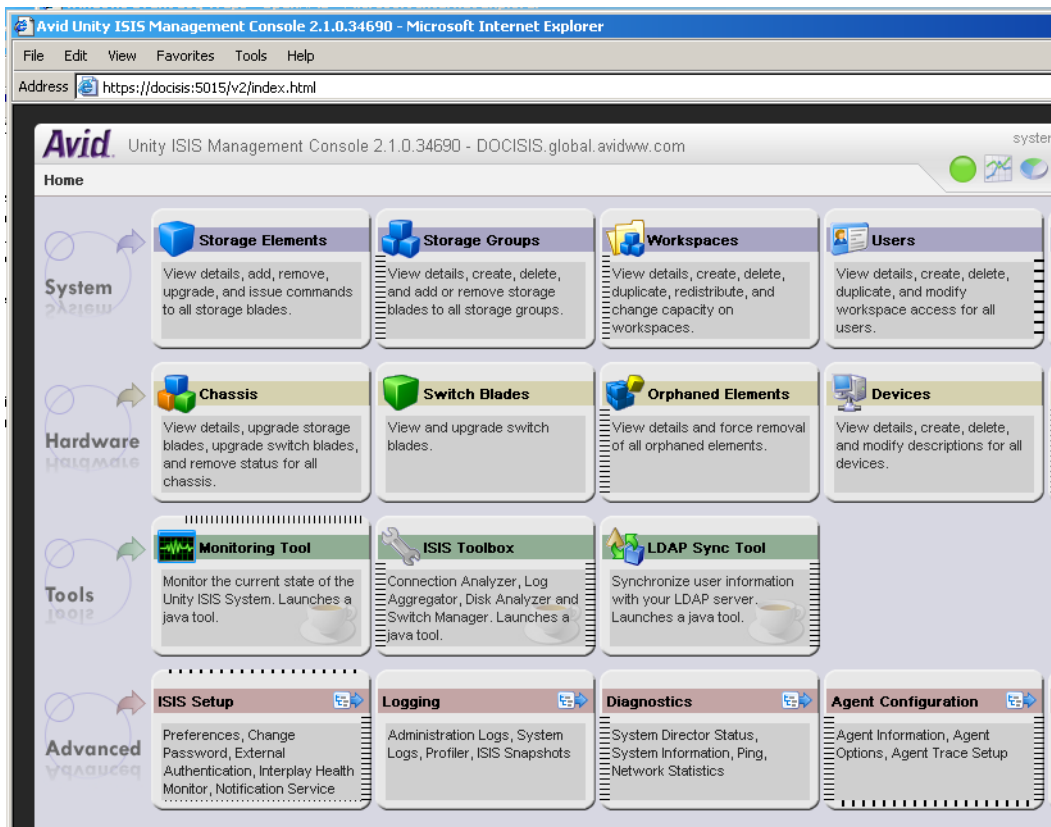
Name:	ISIS Error	
Description:	ISIS Error event	
Parameter:	Name:	Value:
Choose A Path:	Email-Admin ▼	
Text Message:	ISIS Error: %parm[#1]%	
Short Message:	111-%noticeid%	
Email Subject:	ISIS Error: %parm[#1]%	

- Select the email address from the Choose A Path pop-up menu and select Email-Admin.
- Add any descriptive text that makes the email useful to the recipient. There is a list of variables that you can use at the bottom of the window. For additional information, see [“Adding Useful Text to an Email Notification” on page 129](#).
- Click Finish at the bottom of the window.

To test the Event notification:

- Open the ISIS System Director home page.
- In the Advanced row, click Notification Services in the ISIS setup box as shown in the following illustration.

7 Working With Notifications and Maps



 *On an ISIS 5000 system, the Test Subcodes item is grayed out until the Configuration, Filters, and Contacts fields are populated.*

3. Under ISIS Subcode Configuration, select all of the subcode check boxes and click “Test Subcodes”.

Several email notifications will be sent to the email addresses you specified in the Path. Note that a number of events will also be generated in the OpenNMS Recent Event window for the System Director including a number classified as Indeterminate.

4. To stop receiving these events, do one of the following:
 - a. Turn off Notifications globally. See [“Turning Notifications On and Off Globally” on page 121](#).
 - b. Turn off Event notifications for the ISIS Error Event notification.
 - c. Change the path in the ISIS Error Event Notification.



The ISIS Error, Informational, Notification, Success, and Warning notifications each turn on a large group of notifications. Other Notifications such as “Media Indexer Handshake Errors Too High” occur only if one particular event occurs. However, if the event occurs multiple times you will receive multiple emails. So use email notification carefully.

For additional information on configuring ISIS notifications, see [“Modifying Notifications from ISIS” on page 161](#).

Adding Useful Text to an Email Notification

There are a number of variables listed at the bottom of the email notification window such as %nodelabel% which allows you to specify which node has the problem. For example, the following text shows the text with variables and the resulting email.

The number of files being monitoring by Media Indexer %nodelabel% is too high. The current file count is %parm[value]% and the recommended limit is %parm[threshold]%.

**Event: %eventid%
Severity: %severity%
Time: %time%
Node: %nodelabel%
Interface IP: %interface%**

The following text shows sample output from the email.

The number of files being monitored by Media Indexer bpl-flk2mi1 is too high. The current file count is 26555 and the recommended limit is 25000.

Event: 115629
Severity: Minor
Time: Friday, April 23, 2010 6:10:15 PM EDT
Node: bpl-flk2mi1
Interface: 172.20.76.34

Sending Notifications to An External Monitoring System

OpenNMS allows you to send notifications as SNMP traps to an external monitoring system such as LorientPro. You define a separate destination path for each notification you want to send. Several notifications are pre-defined for Avid System Monitor. This section describes how to enable those notifications and how to define additional notifications.

Setting Up the Receiving SNMP Monitoring System

Consult the documentation for your SNMP Monitoring system for details on how to receive traps from another system such as OpenNMS.

We use LorientPro in this example and LorientPro does not require an special configuration to accept traps from another system. The traps appear automatically in the Traps tab in the Event dialog. The following illustration shows several OpenNMS traps appearing in LorientPro. For additional information, see the LorientPro web site: <http://www.lorientpro.com>.

Configuring OpenNMS to Send Traps to the Monitoring System

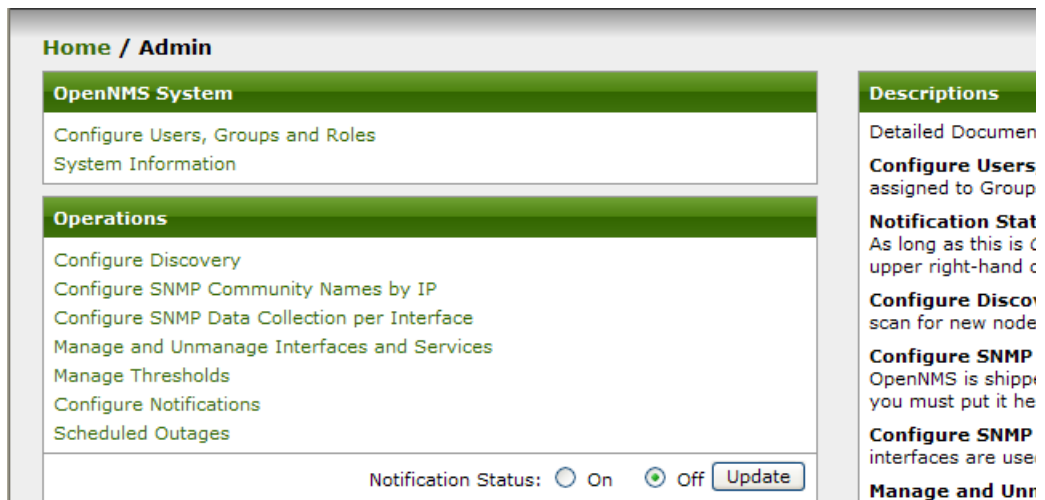
This section assumes that the trap notifications are already defined in OpenNMS. Avid System Monitor defines the following trap notifications for sending to an external monitoring system.

- Avid ISIS SD Active Clients Critical Trap
- Avid ISIS SD Highest Disk Percentage Used Critical Trap
- Avid ISIS SD Number Of Files Critical Trap
- Avid ISIS SD Open Files Critical Trap
- Avid ISIS SD Total Transfer Rate Critical Trap
- Avid ISIS SD Total Used Storage Critical Trap
- Avid ISIS SD Workspaces Critical Trap

You can define additional notifications.

Turning on notifications in OpenNMS:

1. In OpenNMS, click the Admin link.
2. Under Operations click On for Notification Status and then click Update.



3. Click Configure Notifications > Configure Event Notifications. The Event Notifications window opens.
4. Click On for the notifications that you want to send to the external monitoring system.

7 Working With Notifications and Maps

The following illustration shows the notifications that are configured for sending to an external monitoring system. They all end with the text Critical Trap.

Edit	Delete	☒ Off ☐ On	Avid ISIS SD Active Clients Critical Trap	Avid ISIS
Edit	Delete	☒ Off ☐ On	Avid ISIS SD Highest Disk Percentage Used Critical Trap	Avid ISIS
Edit	Delete	☒ Off ☐ On	Avid ISIS SD Number Of Files Critical Trap	Avid ISIS
Edit	Delete	☒ Off ☐ On	Avid ISIS SD Open Files Critical Trap	Avid ISIS
Edit	Delete	☒ Off ☐ On	Avid ISIS SD Total Transfer Rate Critical Trap	Avid ISIS
Edit	Delete	☒ Off ☐ On	Avid ISIS SD Total Used Storage Critical Trap	Avid ISIS
Edit	Delete	☒ Off ☐ On	Avid ISIS SD Workspaces Critical Trap	Avid ISIS



These are the only notifications that are defined to send to an external monitoring system. If you want to add additional notifications you must define them.

5. Make note of the notifications you turned on so you can edit those entries in the notifications.xml file as described in the following procedure.

To Identify the external monitoring system in OpenNMS:

1. Locate the following file on the OpenNMS server and open it in an application such as Wordpad.

Program Files/OpenNMS/etc/notifications.xml

2. Locate a notification you want to send to the external monitoring system and edit the trapHost line for that notification. Replace the value my-trap-host.mydomain.org with the IP address of the external monitoring system.

The following illustration shows the trapHost entry for the Active Clients Critical Traps notification.

```
<notification name="Avid ISIS SD Active Clients Critical Trap" status="on" writeable="yes">
  <uei xmlns="">uei.opennms.org/avid/isis/isisactiveclientcritical-trigger</uei>
  <description xmlns="">The active client count is too high. The number of active client is %parm[value]% while the config
    [threshold]%.</description>
  <rule xmlns="">(IPADDR IPLIKE *.*.*.*)</rule>
  <destinationPath xmlns="">trapNotifier</destinationPath>
  <text-message xmlns="">The active client count is too high. The number of active clients is %parm[value]% and the reco
    [threshold]%. Some clients may be experiencing dropped frames or degraded performance.</text-message>
  <subject xmlns="">Notice #%%noticeid%%</subject>
  <numeric-message xmlns="">111-%%noticeid%%</numeric-message>
  <parameter name="trapVersion" value="v1" />
  <parameter name="trapTransport" value="UDP" />
  <parameter name="trapHost" value="my-trap-host.mydomain.org" />
  <parameter name="trapPort" value="162" />
  <parameter name="trapCommunity" value="public" />
  <parameter name="trapEnterprise" value="1.3.6.1.4.1.5813" />
  <parameter name="trapGeneric" value="6" />
  <parameter name="trapSpecific" value="6" />
  <parameter name="trapVarbind" value="Node: %%nodeid%%. The active client count is too high. The number of active cli
    configured limit is %parm[threshold]%.</parameter>
</notification>
```

3. Edit the corresponding trapHost entry for any additional notifications you want to send to the external monitoring system.



You must edit the trapHost entry for each notification you want to send to the external monitoring system.

4. Save the file and restart OpenNMS.

The next time one of these events is triggered, OpenNMS should send an event to the ISIS node and also send an SNMP trap to the external monitoring system. Refer to the example at the beginning of this section.

Defining Notifications to Send to an External Monitoring System

This section describes how to set up a notification for a specific event. This is a three step process.

- Define the notification in the OpenNMS interface
- Edit etc/notification.xml to complete the notification
- Restart OpenNMS

To define a notification to an external monitoring system:

1. In the OpenNMS interface, select Admin > Configure Notifications > Configure Event Notifications.

The Event Notification window opens.

Home / Admin / Configure Notifications / Event Notifications

Event Notifications

Add a notification to an event or edit an existing event notification

Add New Event Notification

Event Notifications

Actions	Notification	E
EditDelete ☒ Off ☐ On		
EditDelete ☒ Off ☐ On		
EditDelete ☒ Off ☐ On		

2. Click Add New Event Notification The Choose Event
- The Choose Events window opens.

Choose the event uei that will trigger this notification.

Events

Avid Interplay Engine ieClusterAlive Critical Threshold

Avid Interplay Engine ieConnection Warning Cleared

Avid Interplay Engine ieConnection Warning Threshold

Avid Interplay Engine ieDumpFiles Critical Status Cleared

Avid Interplay Engine ieDumpFiles Critical Threshold

Avid Interplay Engine ieJournalFile Critical Status Cleared

Avid Interplay Engine ieJournalFile Critical Threshold

Avid Interplay Engine ieJournalFile Warning Cleared

Avid Interplay Engine ieJournalFile Warning Threshold

Avid Interplay Engine ieLoadedObjects Warning Cleared

Avid Interplay Engine ieLoadedObjects Warning Threshold

Avid Interplay Engine ieLock Critical Status Cleared

Avid Interplay Engine ieLock Critical Threshold

Avid Interplay Engine ieLogSize Critical Status Cleared

Avid Interplay Engine ieLogSize Critical threshold

Avid Interplay Engine ieLogSize Warning cleared

Avid Interplay Engine ieLogSize Warning threshold

Avid Interplay Engine ieLogin Critical Status Cleared

Avid Interplay Engine ieLogin Critical Threshold

Avid Interplay Engine ieLoginTime Critical Status Cleared

Reset

Next >>>

3. Select the event you want to associate with the notification. In this example we select “Avid Interplay Engine ieLogSize Critical Threshold”.
4. Click Next at the bottom of the window.
5. In the next window, click Skip Validation Rules.
- The Choose Path window opens.

Choose path menu

Choose the destination path and enter the information to send via the notification

Name:	Avid IE ieLogSize Critical Threshold Trap													
Description:	Description of this notification													
Parameter:	Name: Value:													
Choose A Path:	trapNotifier ▼													
Text Message:	Text message of this notification													
Short Message:	111-%noticeid%													
Email Subject:	Notice # %noticeid%													
Special Values:	Can be used in both the text message and email subject: <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 33%;">%noticeid% = Notification ID number</td> <td style="width: 33%;">%time% = Time sent</td> <td style="width: 33%;">%severity% = Event</td> </tr> <tr> <td>%nodelabel% = May be IP address or empty</td> <td>%interface% = IP address, may be empty</td> <td>%service% = Service</td> </tr> <tr> <td>%eventid% = Event ID, may be empty</td> <td>%parm[a_parm_name]% = Value of a named event parameter</td> <td>%parm[#N]% = Value index N</td> </tr> <tr> <td>%ifalias% = SNMP ifAlias of affected interface</td> <td>%interfaceresolve% = Reverse DNS name of interface IP address</td> <td>%operinstruct% = Operation event definition</td> </tr> </table>		%noticeid% = Notification ID number	%time% = Time sent	%severity% = Event	%nodelabel% = May be IP address or empty	%interface% = IP address, may be empty	%service% = Service	%eventid% = Event ID, may be empty	%parm[a_parm_name]% = Value of a named event parameter	%parm[#N]% = Value index N	%ifalias% = SNMP ifAlias of affected interface	%interfaceresolve% = Reverse DNS name of interface IP address	%operinstruct% = Operation event definition
%noticeid% = Notification ID number	%time% = Time sent	%severity% = Event												
%nodelabel% = May be IP address or empty	%interface% = IP address, may be empty	%service% = Service												
%eventid% = Event ID, may be empty	%parm[a_parm_name]% = Value of a named event parameter	%parm[#N]% = Value index N												
%ifalias% = SNMP ifAlias of affected interface	%interfaceresolve% = Reverse DNS name of interface IP address	%operinstruct% = Operation event definition												
Finish														

6. Select trapNotifier from the Choose a Path pop-up menu.



The trapNotifier entry identifies the notification as one that will send an SNMP trap to an external monitoring system.

7. In the Name field, enter the text that you want to appear in the Notifications list in the OpenNMS interface.



The name must be less than 63 characters.

8. In the Description area, enter the text that you would like to appear as the subject line for the notification. For additional information, see [“Adding Useful Text to an Email Notification”](#) on page 129.

9. In the Description area, add text that will appear as part of the notification.

10. Click Finish at the bottom of the window.

The Event Notifications window opens.

11. Locate the Notification that you just created and click the On button.

To edit the notification.xml file and complete the notification:

1. On the OpenNMS server, edit the following file in an application such as WordPad:

Program Files/OpenNMS/etc/notification.xml
2. Locate the name of the notification that you created in the OpenNMS interface.

The following illustration shows the Active Clients notification used in this example:

```
- <notification name="Avid IE ieLogSize Critical Threshold Trap" status="on" writeable="yes">
  <uei xmlns="">uei.opennms.org/avid/interplayengine/ieLogSizeCritical</uei>
  <description xmlns="">Description of this notification</description>
  <rule xmlns="">(IPADDR IPLIKE *.*.*.*)</rule>
  <destinationPath xmlns="">trapNotifier</destinationPath>
  <text-message xmlns="">Text message of this notification</text-message>
  <subject xmlns="">Notice # %noticeid%</subject>
  <numeric-message xmlns="">111- %noticeid%</numeric-message>
</notification>
```

3. Add the following parameters after </numeric-message> to complete the trap notification:

```
<parameter name="trapVersion" value="v1" />
<parameter name="trapTransport" value="UDP" />
<parameter name="trapHost" value="my-trap-host.mydomain.org" />
<parameter name="trapPort" value="162" />
<parameter name="trapCommunity" value="public" />
<parameter name="trapEnterprise" value="1.3.6.1.4.1.5813" />
<parameter name="trapGeneric" value="6" />
<parameter name="trapSpecific" value="1" />
<parameter name="trapVarbind" value="Node: %nodelabel%. Actual
value:%parm[value]%, Threshold: %parm[threshold]%" />
```

The following illustration shows the completed section. The trapHost identifies the external monitoring system. You can take this opportunity to specify the IP address of the external monitoring system.

```
- <notification name="Avid IE ieLogSize Critical Threshold Trap" status="on" writeable="yes">
  <uei xmlns="">uei.opennms.org/avid/interplayengine/ieLogSizeCritical</uei>
  <description xmlns="">Description of this notification</description>
  <rule xmlns="">(IPADDR IPLIKE *.*.*.*)</rule>
  <destinationPath xmlns="">trapNotifier</destinationPath>
  <text-message xmlns="">Text message of this notification</text-message>
  <subject xmlns="">Notice # %noticeid%</subject>
  <numeric-message xmlns="">111-%noticeid%</numeric-message>
  <parameter name="trapVersion" value="v1" />
  <parameter name="trapTransport" value="UDP" />
  <parameter name="trapHost" value="my-trap-host.mydomain.org" />
  <parameter name="trapPort" value="162" />
  <parameter name="trapCommunity" value="public" />
  <parameter name="trapEnterprise" value=".1.3.6.1.4.1.5813" />
  <parameter name="trapGeneric" value="6" />
  <parameter name="trapSpecific" value="1" />
  <parameter name="trapVarbind" value="Node: %nodelabel%. Actual value:%pam[value]%, Threshold: %par
</notification>
```

4. (Option) To add additional variables to the TrapVarBind line, see [“Adding Useful Text to an Email Notification”](#) on page 129.
5. Save the file and restart OpenNMS.

Known Problem with Editing an Existing Trap Notification

If you try to edit the existing trap notification through the OpenNMS user interface, after clicking finish, the system inserts a duplicate parameters block in the corresponding section of the notification, in etc/notification.xml. To avoid confusion, edit the file and remove the duplicate parameters block.

The following illustration shows the duplicate parameter block that should be removed.

7 Working With Notifications and Maps

```
- <notification name="Avid ISIS SD Active Clients Critical Trap" status="on" writeable="yes">
  <uei xmlns="">uei.opennms.org/avid/isis/isisactiveclientcritical-trigger</uei>
  <description xmlns="">asdf</description>
  <rule xmlns="">(IPADDR IPLIKE *.*.*.*)</rule>
  <destinationPath xmlns="">trapNotifier</destinationPath>
  <text-message xmlns="">asdf</text-message>
  <subject xmlns="">Notice #%%noticeid%%</subject>
  <numeric-message xmlns="">111-%%noticeid%%</numeric-message>
  <parameter name="trapVersion" value="v2c" />
  <parameter name="trapTransport" value="UDP" />
  <parameter name="trapHost" value="10.0.205.169" />
  <parameter name="trapPort" value="162" />
  <parameter name="trapCommunity" value="public" />
  <parameter name="trapEnterprise" value=".1.3.6.1.4.1.526" />
  <parameter name="trapGeneric" value="6" />
  <parameter name="trapSpecific" value="1" />
  <parameter name="trapVarbind" value="Node: %%nodelabel%" />
  <parameter name="trapVersion" value="v2c" />
  <parameter name="trapTransport" value="UDP" />
  <parameter name="trapHost" value="10.0.205.169" />
  <parameter name="trapPort" value="162" />
  <parameter name="trapCommunity" value="public" />
  <parameter name="trapEnterprise" value=".1.3.6.1.4.1.526" />
  <parameter name="trapGeneric" value="6" />
  <parameter name="trapSpecific" value="1" />
  <parameter name="trapVarbind" value="Node: %%nodelabel%" />
</notification>
```

Working with Maps

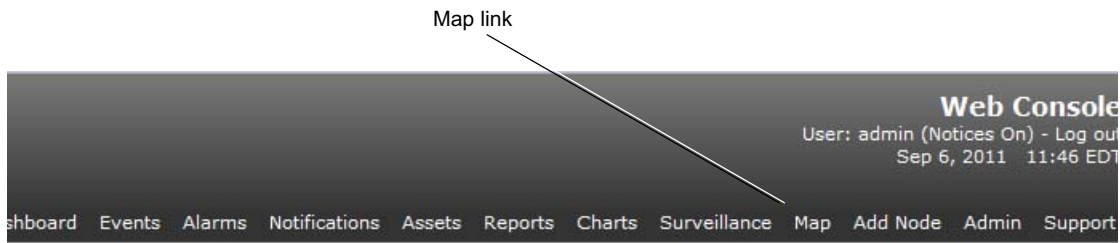
This section describes how to turn on the map feature and describes the basics of creating maps.

Turning on the Map Feature

To turn on the map feature:

1. Navigate to the following directory on the OpenNMS server:
Program Files\OpenNMS\etc
2. Locate the file map.disable.
3. Change the name of the file to map.enable.
4. Restart the Avid Monitoring Service. See [“Restarting or Stopping OpenNMS”](#) on page 51.

The Map link appears next to the Admin link when you re-log onto the OpenNMS web interface.



Showing Switch Connectivity

If you add LAN switches to your map you can display the connections between the switch and other nodes.

To enable connectivity display:

1. Locate the following file and open it in an application such as WordPad or an xml editor:

\etc\service-configuration.xml

2. Uncomment the following lines:

```
<service>
    <name>OpenNMS:Name=Linkd</name>
    <class-name>org.opennms.netmgt.linkd.jmx.Linkd</class-name>
    <invoke at="start" pass="0" method="init"/>
    <invoke at="start" pass="1" method="start"/>
    <invoke at="status" pass="0" method="status"/>
    <invoke at="stop" pass="0" method="stop"/>
</service>
```

3. Save the file and restart the OpenNMS service.

Installing the Adobe SVG Viewer

Some browsers require that you install the Adobe SVG viewer to view maps. OpenNMS prompts you to install the viewer if it is required. If you are connected to the internet, you can usually complete the install while you are still using the OpenNMS application. This section describes how to download the viewer if necessary.

To install the Adobe SVG (scalable vector graphics) viewer:

1. Download the installer from Adobe's web site:
<http://www.adobe.com/svg/viewer/install/>
2. Install the viewer software.

Known Problems with the Map Feature

The Maps feature is useful for a visual representation of the environment but creating maps can be a challenge. There are a number of limitations related to working with the Maps feature as follows:

- When creating and modifying maps, testing has shown that Mozilla Firefox works better than Internet Explorer. Users can view maps with Internet Explorer but creating and modifying them in Firefox is recommended.
- The Node > Add Category and Node > Add Label commands do not work as expected. Adding nodes one at a time is more reliable.
- For best results, rename and save a new map as soon as you create it.

See the Avid System Monitor Readme for additional information.

Creating a New Map

To create a map:

1. Click Map on the OpenNMS top level interface.
2. Select Map > Admin Mode.
3. Do the following to create a map:
 - a. Select Map > New.
 - b. Select Map > Rename and name the node.
 - c. Select Map > Save.

OpenNMS displays the name of the new map on a tab.

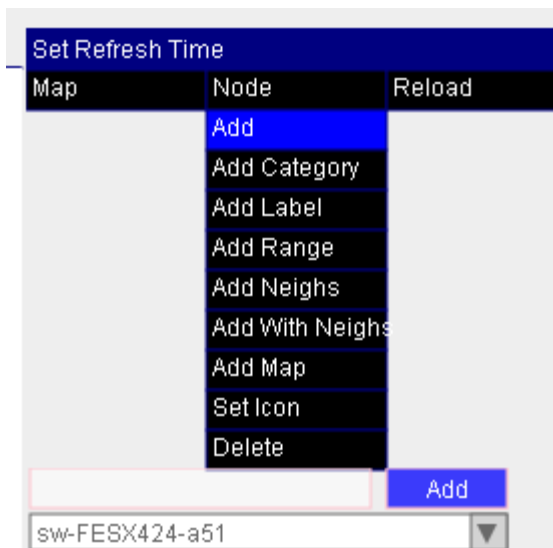


Renaming and then saving the map are important steps for creating a map.

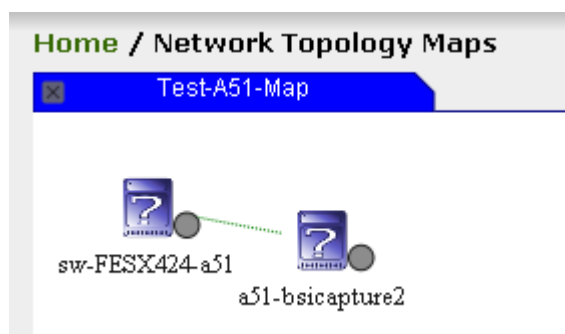
4. Select Node > Add.



Use Node Add. Add Category and Add Label do not work correctly for this release. See the Avid System Monitor Readme for additional information.



5. Select a node from the list and click Add. The following illustration shows two nodes added: a Foundry switch and a second Interplay Capture node named a51-bsicapture2. The system displays the connection between the switch and the Interplay Capture system. See [“Showing Switch Connectivity”](#) on page 139.



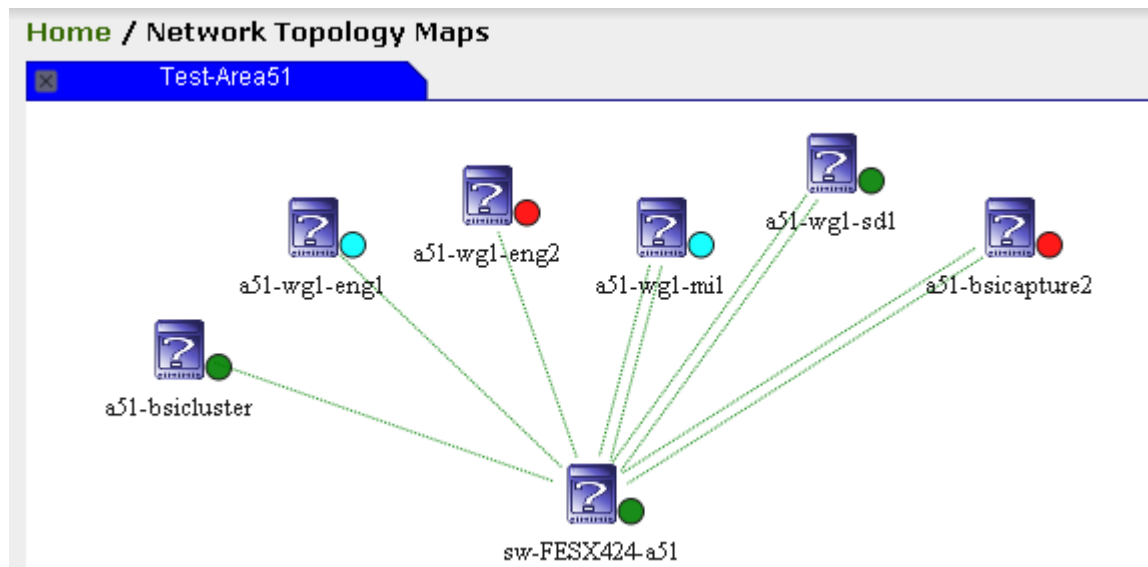
6. Add additional nodes as required.
7. Select Map > Save to save your work.



It is important to save before you use the next command to display the status colors.

8. Select Reload > Config. OpenNMS updates the connectivity and shows appropriate colors for the status of each node.

The following illustration shows several nodes added. In this example all of the nodes are connected to the same switch.

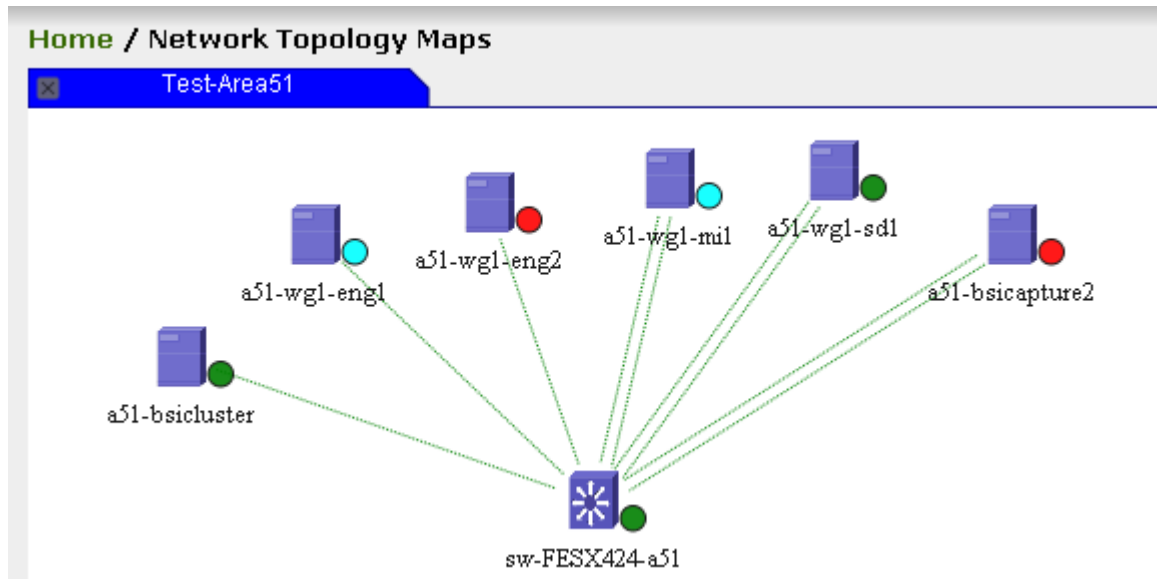


9. To replace the default icons, select Node > Admin Mode and then select Node > Set Icon.
10. Select an icon from the list, and click the node you want to change. You can click multiple nodes to change several icons in the same operation.
11. Click Map > Save and then click Reload > Config.



Save any changes before you use the Reload Config command.

The following illustration shows the completed map.



Adding a Background Graphic

You can add a background graphic to organize the nodes in a map. For example, you could arrange the nodes in the relative positions they occupy in your lab. Maps are .jpg files and are located in the following directory (assuming an install on the D:\ drive.)

D:\Program Files\OpenNMS\jetty-webapps\opennms\map\images\background

The default backgrounds are geographical maps but you can create your own backgrounds for your site.

To add a custom background image:

1. Save the image as a .jpg file and copy it to the following folder (assuming an installation on the D:\ drive):
D:\Program Files\OpenNMS\jetty-webapps\opennms\map\images\background
2. Open the map.properties file in the OpenNMS\etc directory.
3. Locate the Background Images section.
4. Add the name of your file in two locations as shown in the following example. There are two custom images in this example: warroom.jpg and 10geLAN.jpg.

The following illustration shows the custom names added to the map-properties file.

```
#####  
## BACKGROUND IMAGES  
#####  
# A comma-separated list of bgimages keys.  
# bgimages.{KEY}.filename  
bgimages=warroom,10geLAN,napoli,italia,abruzzo,basilicata,calabria,campania,emilia_romag  
  
bgimage.warroom.filename=warroom.jpg  
bgimage.10geLAN.filename=10geLAN.jpg  
bgimage.napoli.filename=napoli.gif  
bgimage.italia.filename=italia.jpg  
bgimage.abruzzo.filename=abruzzo.jpg  
bgimage.basilicata.filename=basilicata.jpg  
bgimage.calabria.filename=calabria.jpg  
bgimage.campania.filename=campania.jpg
```



Maintain the files in the same order in both lists. For example, put both entries at the beginning of its corresponding list.

5. Save the file and restart the OpenNMS service.
6. Open your map in OpenNMS.



Start off using the Dimension > Auto setting on the Map selection page and then experiment with different resolutions.

7. Select Map > Admin and then select Map > Set Background > Image
8. Select the image from the list and click Set.
9. Rearrange the nodes on the background.
10. Select Map > Save to save your changes.

Opening an Existing Map and Viewing Node Status

To open an existing map:

1. Click Map on the OpenNMS menu list.
2. Select the Map name from the Open Map menu and click View.

OpenNMS opens the map. The state of each node is displayed via a color dot. For the list of color states, see the Severity view on the map legend.

3. To see additional information on each node, do the following:

- Select a node and view the node up/down status, availability, and severity level in the map legend area.
- Right-click the node and select Ping, Traceroute, Events, or Resource Graphs information. If you select Resource Graphs, choose Node Level Data if it is available.
- Double-click the node to open the page for that node in a separate window.

8 Working with OpenNMS

This section describes some of the day to day uses of the Avid System Monitor. It also describes some things to do if you are aware of a problem in your Interplay environment and you want to use OpenNMS and the Avid System Monitor to identify the problem.

- [Changing Threshold Values](#)
- [Troubleshooting](#)
- [Working with Resource Graphs](#)
- [Creating Reports](#)
- [Removing Discovered Services from a Node](#)
- [Working with Alarms](#)
- [Running the Avid System Monitor Upgrade Utility](#)
- [Backing Up and Restoring Avid System Monitor](#)
- [Restoring an Avid System Monitor Backup](#)

Changing Threshold Values

There are times when you will need to fine tune some threshold values to match the needs of your site. In addition, there are some values that you should change depending on the version of the corresponding application. The following table lists values that you may want to change.

Node	Value	Default Warning and Critical Threshold	Threshold Value Name (Datasource)
Interplay Engine	Log file size	10 MB change (10 million bytes)	ieLogSize
	Media deletes and metadata deletes	10,000	ieMediaDeletes, ieMetaDeletes
	Total objects in database ^a	40 million/50 million	ieTotalObjects
	Number of used Interplay licenses	150/200	ieUsedLicenses
Stream Server ^b Make these changes for Interplay v2.4 and later.	Bandwidth Note: 700 million translates to 700 MBit	700 million/800 million change to: 500 million/600 million and rearm at 500 million	issBandwidth
	Application Status	3 is critical value Change rearm value to 1 (stands for OK)	issStatus
	Connections (number of current streams)	250/500 change to 90/105 and rearm at 80	issConnection
	Number of current sessions	250/500 change to 350/500 and rearm at 300	issSessions
	Is the Share available	Delete this threshold for Interplay v2.4 and greater^c	issShareAvail
Media Indexer	Number of Unique Media Files	2.4 million Change to 250K for 32-bit MI and 2.4 million for 64-bit MI	AIMIUniqueMediaFil

Node	Value	Default Warning and Critical Threshold	Threshold Value Name (Datasource)
Interplay Capture	Number of Handshake errors	16 change to 4 for MI versions earlier than v2.1.1	AIMIHandshake
	Page File Size	Delete this threshold on Avid System Monitor v1.0 systems.	AIMIPageFileUsage
	Memory Usage	Delete this threshold on Avid System Monitor v1.0 systems.	AIMIMemoryUsage
	Redundancy group size	If you only have one Capture server you can delete this threshold. Sites usually have two for redundancy.	ACSRedundancyGrpSz
Lookup Service	Thread Count ^d	1300/800 Change to 2000/1800	ALUThreadCount
	Handle Count	17000/15000 Change to 25000/23000	ALUHandleCount
ISIS System Directors	Number of active clients	ISIS 5000 37 ISIS 7000 320 Adjust this depending on the number of active clients recommended for your ISIS configuration.	ISISActiveClientCnt
	ISIS Bandwidth	ISIS 5000: 550 MB/sec ISIS 7000: 4.8GB This value is dependent on a number of variables including the number of ISIS crates, the working resolution, and number of streams per client used at your site.	ISISMBPerSec
	Percentage of available storage space used	90% No need to change	ISISTotalUsedMB
	Combined file and folder count.	ISIS 5000: 3 million ISIS 7000: 10 million No need to change	ISISFileCount + ISISFolderCount

Node	Value	Default Warning and Critical Threshold	Threshold Value Name (Datasource)
	Trigger when any disk gets this full	90% No need to change	ISISHighestDiskUsed
	Number of workspaces	800 No need to change	ISISWorkspaceCount
	Number of open files	50,000 No need to change	ISISOpenFiles

- a. See “Number of Objects in the Interplay Database” on page 157.
- b. See “Changes for the Stream Server” on page 152.
- c. Interplay v2.4 and greater does not require a share for the Streaming Server so this threshold value should be deleted.
- d. See “Handle Count and Thread Count” on page 157.

For example, if you have 100 Interplay licenses, you can change the threshold values to something like 80 for a warning and 95 for critical.

To change the warning threshold for the number of Interplay licenses:

1. In the OpenNMS interface, click Admin.
2. Under Operations, click Manage Thresholds.

The Threshold Groups window opens.



3. Locate the Threshold Configuration name that you want to modify. In this case it is AvidInterplayEngine.
4. Click the corresponding Edit button on the right side of the window.
5. The Edit Group window opens.

6. Scroll down to the Datasource value you want to modify the threshold for. In this case, locate ieUsedLicenses. The low values are for the Warning threshold and the high values are for the Critical threshold.

Used Licenses value

high	ieTotalObjects	node	5000000.0	5
low	ieLoadedObjects	node	1000.0	1
high	ieLoginTime	node	30000.0	5
high	ieUsedLicenses	node	150.0	1
high	ieUsedLicenses	node	200.0	2
high	ieBackupDuration	node	300.0	3
high	ieBackupDuration	node	250.0	2

7. Click the corresponding Edit button on the right side of the window.
- The Edit Threshold window opens.

USER: admin

AP

st Search Outages Path Outages Dashboard Events Alarms Notifications Assets Reports Charts Surveillance

Group / Edit Threshold

Datasource type	Datasource label	Value	Re-arm
	node	150.0	150.0

8. Change the Value to the new trigger threshold value you want to use. In this case the trigger and rearm values are the same so change the re-arm value to the same value.
9. Click Save.
10. Restart the Avid System Monitoring service.

Known Problems with Notifications for the Interplay Engine and Stream Server

Testing has shown that the following thresholds may create unnecessary notifications:

- Avid Interplay Engine ieLoadedObjects
- Avid Interplay Engine ieStatus
- Avid Interplay Stream Server issStatus

Avid recommends that you disable these notifications.

To turn off notifications for the Interplay Engine SNMP agent:

1. Select Admin > Configure Notifications > Configure Event Notifications
2. Click Off for the notifications as shown in the following illustrations.

Edit	Delete	☒ Off ☐ On	Avid Interplay Engine ieLoadedObjects Warning Cleared
Edit	Delete	☒ Off ☐ On	Avid Interplay Engine ieLoadedObjects Warning Threshold
Edit	Delete	☒ Off ☐ On	Avid Interplay Engine ieStatus Critical Status Cleared
Edit	Delete	☒ Off ☐ On	Avid Interplay Engine ieStatus Critical Threshold
Edit	Delete	☒ Off ☐ On	Avid Interplay Engine ieStatus Warning Cleared
Edit	Delete	☒ Off ☐ On	Avid Interplay Engine ieStatus Warning Threshold
Edit	Delete	☒ Off ☐ On	Avid Interplay Stream Server issStatus critical status cleared
Edit	Delete	☒ Off ☐ On	Avid Interplay Stream Server issStatus critical threshold
Edit	Delete	☒ Off ☐ On	Avid Interplay Stream Server issStatus warning status cleared
Edit	Delete	☒ Off ☐ On	Avid Interplay Stream Server issStatus warning threshold

This will turn off event notifications for these items. If you have email notifications turned on, this will avoid unnecessary email notifications.



Each time you click an On or Off button the OpenNMS interface jumps to the top of the window and you must scroll down to click the next item.

Changes for the Stream Server

For Interplay Stream server v2.4 and later you should delete the threshold value that checks whether the share is available. The share is no longer used starting at Stream Server v2.4. There are also a number of threshold values that should be changed. See [“Changing Threshold Values”](#) on page 148.



The procedures in this section are advanced and can affect the performance of the Avid System Monitor. Before you begin modifying the thresholds on your system you should perform a complete backup of the OpenNMS files and PostgreSQL database. Then you can easily return to your original configuration. See [“To Perform a Complete Backup of Avid System Monitor”](#) on page 192.

The following illustration shows the threshold values that should be changed or deleted. Note that for a large value like 800 million, you enter the full number 800000000 and the system automatically saves the value as 8.0E8.

	Type	Datasource	Datasource type	Datasource label	Value	Re-arm	Trigger
Critical status	high	issStatus	node		3.0	2.0	1
	high	issCPULoad	node		75.0	75.0	1
Bandwidth critical	high	issBandwidth	node		8.0E8	8.0E8	1
Connections critical	high	issConnection	node		500.0	500.0	1
Sessions critical	high	issSessions	node		500.0	500.0	1
No change	high	issStatus	node		2.0	1.0	1
Delete	low	issShareAvail	node		0.0	0.0	1
Bandwidth warning	high	issBandwidth	node		7.0E8	7.0E8	1
Connections warning	high	issConnection	node		250.0	250.0	1
Sessions warning	high	issSessions	node		250.0	250.0	1

You can tell whether a value such as issBandwidth corresponds to a critical or warning threshold by looking at the value at the end of the corresponding Re-armed UEI string. The following illustration shows the warning and critical values for issBandwidth.

Re-armed UEI		
uei.opennms.org/avid/streamingserver/issStatusCritical-rearm	Edit	Delete
uei.opennms.org/avid/streamingserver/issCPULoad-rearm	Edit	Delete
uei.opennms.org/avid/streamingserver/issBandwidthCritical-rearm	Edit	Delete
uei.opennms.org/avid/streamingserver/issConnectionsCritical-rearm	Edit	Delete
uei.opennms.org/avid/streamingserver/issSessionsCritical-rearm	Edit	Delete
uei.opennms.org/avid/streamingserver/issStatusWarn-rearm	Edit	Delete
uei.opennms.org/avid/streamingserver/issShareAvail-rearm	Edit	Delete
uei.opennms.org/avid/streamingserver/issBandwidthWarn-rearm	Edit	Delete
uei.opennms.org/avid/streamingserver/issConnectionsWarn-rearm	Edit	Delete

Critical

Warning

To delete the issShareAvail (share available) threshold:

1. Select Admin > Manage Thresholds.
2. Locate AvidStreamingServer and click Edit on the right side of the window.
3. In the DataSource column, locate issShareAvail.
4. Click the Delete button on the far right. To make sure you delete the correct threshold, check that the corresponding re-armed UEI string ends with issShareAvail-rearm.
5. Restart the Avid System Monitor service.

To edit the Stream Server bandwidth critical threshold:

1. Select Admin > Manage Thresholds.
2. Locate AvidStreamingServer and click Edit on the right side of the window. The Edit group AvidStreamingServer window opens and displays the available threshold values.
3. Locate the top issBandwidth datasource value and scroll to the right to locate the corresponding Edit button. To make sure you edit the correct threshold, check that the corresponding Re-armed UEI string ends with issBandwidthCritical-rearm.

Re-armed UEI		
uei.opennms.org/avid/streamingserver/issStatusCritical-rearm	Edit	Delete
uei.opennms.org/avid/streamingserver/issCPULoad-rearm	Edit	Delete
uei.opennms.org/avid/streamingserver/issBandwidthCritical-rearm	Edit	Delete
uei.opennms.org/avid/streamingserver/issConnectionsCritical-rearm	Edit	Delete

4. Click the Edit button.
- The system displays the Edit threshold window.

Edit threshold

Type

Datasource

Datasource type

high

issBandwidth

Node

Triggered UEI

Re-armed UEI

uei.opennms.org/avid/streamingserver/issBandwidthCritical

uei.opennms.org/avid/stream

Save

Cancel

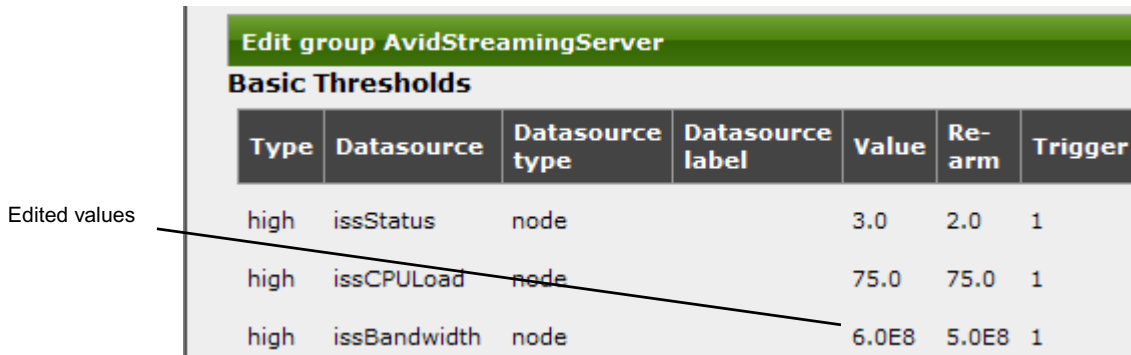
5. Scroll to the right to display the Value and Re-arm text boxes.

Datasource label	Value	Re-arm	Trigger
	8.0E8	8.0E8	1

6. Replace the Value entry 8.0E8 with 600000000 (600 million).
7. Replace the Re-arm entry with 500000000 (500 million).

Datasource label	Value	Re-arm	Trigger
	600000000	500000000	1

8. Scroll to the left and click Save. The system displays the values you entered in scientific notation.



Edit group AvidStreamingServer						
Basic Thresholds						
Type	Datasource	Datasource type	Datasource label	Value	Re-arm	Trigger
high	issStatus	node		3.0	2.0	1
high	issCPULoad	node		75.0	75.0	1
high	issBandwidth	node		6.0E8	5.0E8	1

9. Change any other threshold values as necessary and then restart the Avid System Monitor service.

Changing the Text Notifications for the Stream Server

After you change the threshold values you should also change the text for the corresponding event messages. The v1.2.1 version of the Stream Server notifications contain static values such as 800 or 250. The following procedure describes how to change the notification values to a variable. This ensure that the actual threshold value will be displayed in the message.

To change the threshold text notifications for the Stream Server:

1. Navigate to the following folder:
OpenNMS\etc\events
2. (Option) Make a backup copy of the file AvidStreamingServer.events.xml.
3. Open AvidStreamingServer.events.xml with a text editor such as WordPad.
4. Search for the first occurrence of the string “exceed” that contains a specific numeric value. For example:

...Stream Server: The network bandwidth of the stream server process has exceeded 800 Mbit ...
5. Replace the numeric value with (%parm[threshold]%) including the parentheses. This ensures that the actual threshold value will be displayed. The example should now read as follows:

...Stream Server: The network bandwidth of the stream server process has exceeded (%parm[threshold]%) Mbit ...
6. Continue to search for “exceed” and change the other numeric values to the variable.
7. Save the file and restart the Avid System Monitor service.

Number of Objects in the Interplay Database

To determine a threshold for the number of objects in the Interplay database, check the number when you first install the Avid System monitor. Then set the threshold value to 50% higher than the number of objects in your database.

You can check the total number of database objects by starting the Interplay Administrator client and opening the “Database Information” page. For additional information, see “Viewing Database Information” and “Limits on the Number of Assets and Objects in the Interplay Database” in the Interplay Help or *Interplay Engine and Interplay Archive Engine Administration Guide*.

Handle Count and Thread Count

A number of the monitored applications have threshold values for Handle Count and Thread Count. You should not change these values unless instructed to do so by Avid customer support. Values vary depending on the application and you can view the values on the Edit Threshold page for the application.

Thread count and handle count control how many separate processes an application can handle at the same time. For example, how many simultaneous recordings can be controlled by Interplay Capture. Each thread uses a specific amount of virtual address space and if there are too many threads the application can start to have performance-related problems. In general, if you see an event that states the thread count or handle count is high, you should restart the application at a convenient time. If the problem continues there could be a problem with the application or it could be that the threshold value has been set too low. Check with your Avid representative for additional information.

Troubleshooting

This section assumes that you are aware of a problem in your Interplay environment and you want to use OpenNMS and the Avid System Monitor to determine what is wrong.

Examine the Home Page and Dashboard

Examine the Home page and Dashboard for outages, events, alarms, and notifications. This will give you a quick history of the issues that OpenNMS has been monitoring and may give you some direction as to which systems you need to look at more carefully. Note when the problems occurred so you can examine the resource graphs for those time periods.

For example, the following illustration shows the Main page.

Outage table

Availability

x out of y services are down

Performance and notification

Categories	Outages	Availability
ISIS System Directors	0 of 0	100.000%
Ingest and Playback	0 of 0	100.000%
Interplay Database Engines	0 of 0	100.000%
Interplay Providers	0 of 0	100.000%
Interplay Services	0 of 0	100.000%
LAN Gateways	0 of 0	100.000%
Network Services - AD, DNS, DHCP	0 of 0	100.000%
Total	0 of 73	99.953%

Outages	Availability
0 of 73	99.953%

Notification

You: No outages
All: No outages
On-Call Scheduler: No outages

Resource Group

-- Choose A

KSC Report

No KSC report

In above illustration, there are 10 outages in the Interplay category. The following illustrates several ways to get information about the outages:

- Check the list on the left side of the page for nodes that have outages. For example, the node labeled Stream Server has an outage. This can give you an indication immediately about which services are having problems. Click on that node to get additional information.
- Click the Outages button along the top of the OpenNMS interface. This page presents a summary of the outages that are occurring in the environment. Once you get to the page you can click on Current Outages or All Outages.
 - The All Outages selection looks back in time, You can see outages that have occurred and which nodes have recovered from the outages.
 - Current Outages are the most relevant. Outages are shown by interface as shown in the following illustration. The page shows the different services for each interface on the node and shows the time that the service was down. You can click on the service to get additional information about the outage and you can click on the interface ID or the node name to open the pages for the interface or the node.

Home / Outages / Current By Node			
View All Outages Query Current Outages			
Current Outages			
Node	Interface	Service Down	Time Down
Copy Provider bpl-movecopy	172.20.107.184	ICMP	4/19/10 10:00:0
		StrafePing	4/19/10 10:00:0
	172.20.76.2	SNMP	4/8/10 18:07:12
		Win32AvidUnityISISAdminServer	4/8/10 18:00:51
		Win32AvidUnityISISSystemDirector	4/8/10 18:01:46
		Win32Server	4/8/10 18:01:02
		Win32Time	4/8/10 18:01:13
	172.20.77.2	SNMP	4/8/10 18:02:11
		Win32AvidUnityISISAdminServer	4/8/10 18:05:56
		Win32AvidUnityISISSystemDirector	4/8/10 18:01:36
		Win32Server	4/8/10 18:02:21
		Win32Time	4/8/10 18:01:26

Examine the Resource Graphs

When you determine which categories of devices are having problems, look at the resource graphs for some of those systems and see if you can determine any spikes or trends that will help you narrow down the problem.

The following are some tips for using the graphs:

- Look at the graphs for a node over the last week or during a specific time period. Then drill down for finer details. Once you notice a time period with issues, search for events and alarms during that time period. For systems running the Monitoring Gateway such as Media Indexer, select “Node-level Performance Data” at the top of the window under SNMP node Data. Node Level Performance Data is also available on the Interplay Engine and Stream Server.
- System running the Monitoring Gateway display much of the information that the Health Monitor collects in the Resource Graphs. The advantage is that the values are collected over time and you can look for trends.
- Also check the local drive utilization and physical memory usage for issues. Select the “Storage (MIB-2 Host Resources)” options at the bottom of the Resource Graph window

- View resource graphs on the node for SNMP node and interface data and response times. Check bandwidth utilization, discards and errors. Look for spikes over time and check ICMP and StrafePing response during that time period.
- You can also check resource graphs for switches. You can locate the switch in the Node List. The system will usually have the fully qualified domain name. Also check the main page for the switch. Besides checking for events you can click View Node Link Detailed Info under General near the top of the switches node page. This will give an up/down status on all the interfaces on the switch.

Keep in mind that graphs auto-scale and report decimal values using “u” and “m” values. These may appear to be spikes but are actually very low values. OpenNMS polling also causes a pattern of these low level spikes. Make note of the actual values so that you don’t interpret a small spike as a larger issue. Serious spikes on the system will often show up on a number of graphs at the same time period.

Solving Configuration Problems

The following are some recommendations if services and graphs are not appearing for monitored nodes.

- For the OpenNMS server and for monitored nodes, disable any unused NICS and make sure that the active NICs are at the top of the binding order.
- Make sure that forward and backward DNS lookup is working for any nodes that are not reporting the correct services or graphs. For systems running the Avid Service Framework, you can use the System Check feature in the Workgroup Properties tool.
- If you are using provisioning groups and the node doesn’t appear in the node list after several minutes, it may be useful to delete the associated provisioning group file and start again with a fresh file. See the following section for a procedure to copy a new file from the Avid System Monitor installer DVD.

For additional information, see [“Working with Resource Graphs” on page 163](#).

Fixing a Problem When Provisioning Groups Nodes Don’t Appear

There is a known problem with configuring nodes with Provisioning Groups. Occasionally importing the provisioning group file (in the openNMS user interface) does not add the nodes to the OpenNMS database.

If none of the nodes in the group were added, you can delete the existing provisioning group file and replace it with a default template from the installers folder. The template files are in the `\etc\imports` directory and are named after the provisioning group. For example, the ISIS-SD template is `/etc/imports/ISIS-SD.html`.

To replace a provisioning groups file with the original version:

1. Delete the edited template file in the Program Files\OpenNMS\etc directory. For example, delete imports-ISIS-SD.html. The entry will be automatically removed from the OpenNMS Admin/Provisioning Groups window.
2. Copy the corresponding template file from the \opennms_config\etc folder on the Avid System Monitor Installer and paste it into the Program Files\OpenNMS\etc folder.
3. In OpenNMS, select Admin > Manage Provisioning Groups. The template file should now be displayed in the Admin/Provisioning Groups window.
4. Edit the file and add your provisioning group information.
5. Click Done in the Provisioning Groups/Edit window and click Synchronize for the corresponding provisioning group. The Provisioning group display should now show two numbers for the provisioning group. For example, 2/2 for ISIS-SD.

Modifying Notifications from ISIS

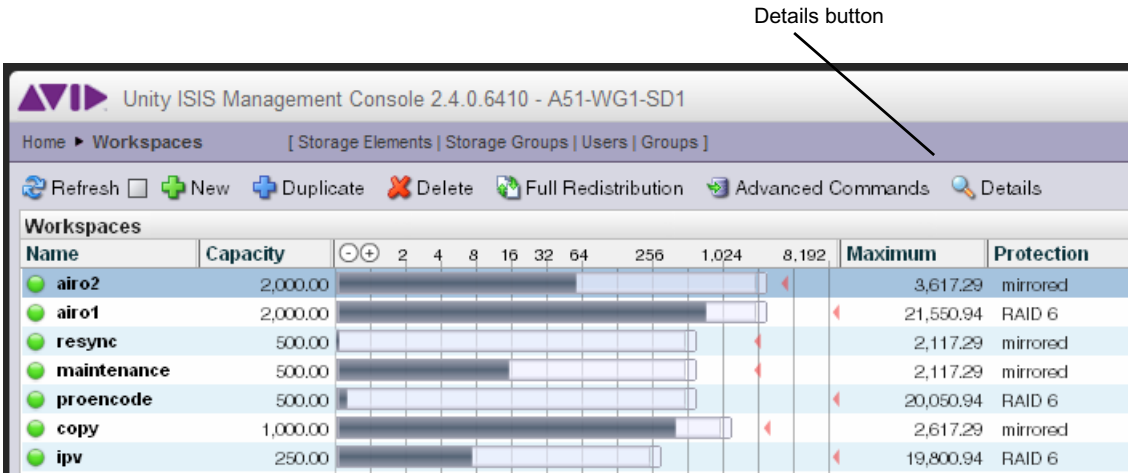
If you turn on notifications for ISIS errors, warnings, and information, OpenNMS will send notifications whenever the ISIS System Director writes a warning or error to the Windows Event log. The following sections describe the feature:

- [“Configuring the ISIS System Director” on page 68](#)
- [“Turning on Notifications and Specifying a Target Email Address” on page 125](#)

When you enable the feature, the ISIS System Director will send a notification when a workspace is full. You can fine tune this information so that ISIS will send a notification when a particular workspace reaches a percentage full or when it reaches a specific MB limit. This can help avoid disk space problems before they occur. ISIS already has the built in functionality for this. This section describes how to enable it in ISIS v2.x.

To configure ISIS to send a notification for a workspace disk space percentage:

1. Log onto the System Director and System > Workspaces.
2. Select the workspace you want to configure and click Details along the top menu bar.



ISIS displays the workspace Details window.

- Configure the percentage values or amount of disk space used values. The following illustration configures ISIS to send a warning when the workspace becomes 80% full and an error when the workspace is 90% full. The error is displayed as a critical event in OpenNMS.

▼ Details

Name	airo2		
Storage Group	storage group ▼		
Protection	mirrored ▼		
Capacity	2,000.00	3,617.29 GB	
Used	55.99 GB		
Reserved	56.04 GB		
Unused	1,944.00 GB		
Files	620		
Directories	31		
Config Changes	0		
Status			
Warning Event Trigger	80	% ▼	used
Error Event Trigger	90	% ▼	used
Chunk Size	512 KB		

- Click Apply in the ISIS interface.



This feature is enabled on an individual workspace basis.

Working with Resource Graphs

This section describes how to display Resource Graphs. To learn how to combine specific graphs into a report, see [“Creating Reports” on page 167](#).

Displaying Resource Graphs

Use the following procedure to display the resource graphs for a node.

To display resource graphs:

1. Open the Node Details page for a node. For example, locate the node in the Node List and click on it.

Home / Search / Node
Node: b3-sd02b.global.avidww.com
Foreign Source: ISIS-B3

[View Events](#) [View Alarms](#) [View Outages](#) [Asset Info](#) [Site Status](#) [Resource Graphs](#) [Rescan](#) [Admin](#) [Schedule](#)

SNMP Attributes	
Name	B3-SD02B
Object ID	.1.3.6.1.4.1.311.1.1.3.1.2
Location	
Contact	
Description	Hardware: EM64T Family 6 Model 15 Stepping 11 AT/AT COMPATIBLE - Software: Windows Version 5.2 (Build 3790 Multiprocessor Free)

Availability	
Availability (last 24 hours)	100.000%
Overall	100.000%
ICMP	100.000%
SNMP	100.000%

General (Status: Active)

[View Node IP Route Info](#)
[View Node Link Detailed Info](#)

Surveillance Category Membe

ISIS System Directors
 Scalar Lab

Notification

You: Outstanding: [\(Check\)](#)
 You: Acknowledged: [\(Check\)](#)

Recent Events

☐ 153273	8/26/11 14:33:47
---------------------------------	------------------

2. Click on Resource Graphs. OpenNMS displays the Node Resources page.
3. Either drag or double click on the items you want to graph. OpenNMS moves the selections to the Select Resources to Graph panel.

8 Working with OpenNMS

Home / Reports / Resource Graphs / Choose
Node: b3-sd02b.global.avidww.com

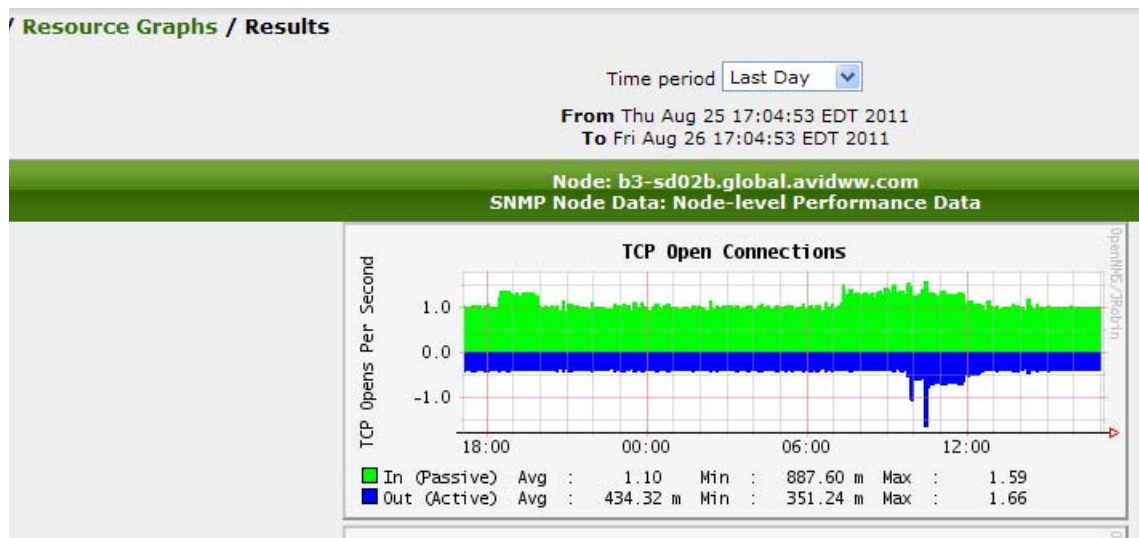
Node Resources

Resources	Selected Resources
Node-level Performance Data	Node-level Perform
Intel(R) PRO/1000 EB Network Connection with I/O Acceleration #2. (192.16...	C:\ Label:Boot Ser
Intel(R) PRO/1000 EB Network Connection with I/O Acceleration. (192.168.1...	Physical Memory
Intel(R) PRO/1000 PT Dual Port Server Adapter #2. (10.104.108.4, 1 Gbps)	
Intel(R) PRO/1000 PT Dual Port Server Adapter. (10.104.100.4, 1 Gbps)	
10.104.100.3	
10.104.100.4	
10.104.108.3	
10.104.108.4	
C:\ Label:Boot Serial Number ccd05bc8	
D:\ Label:Data Serial Number 4c040bc0	
E:\	
Physical Memory	

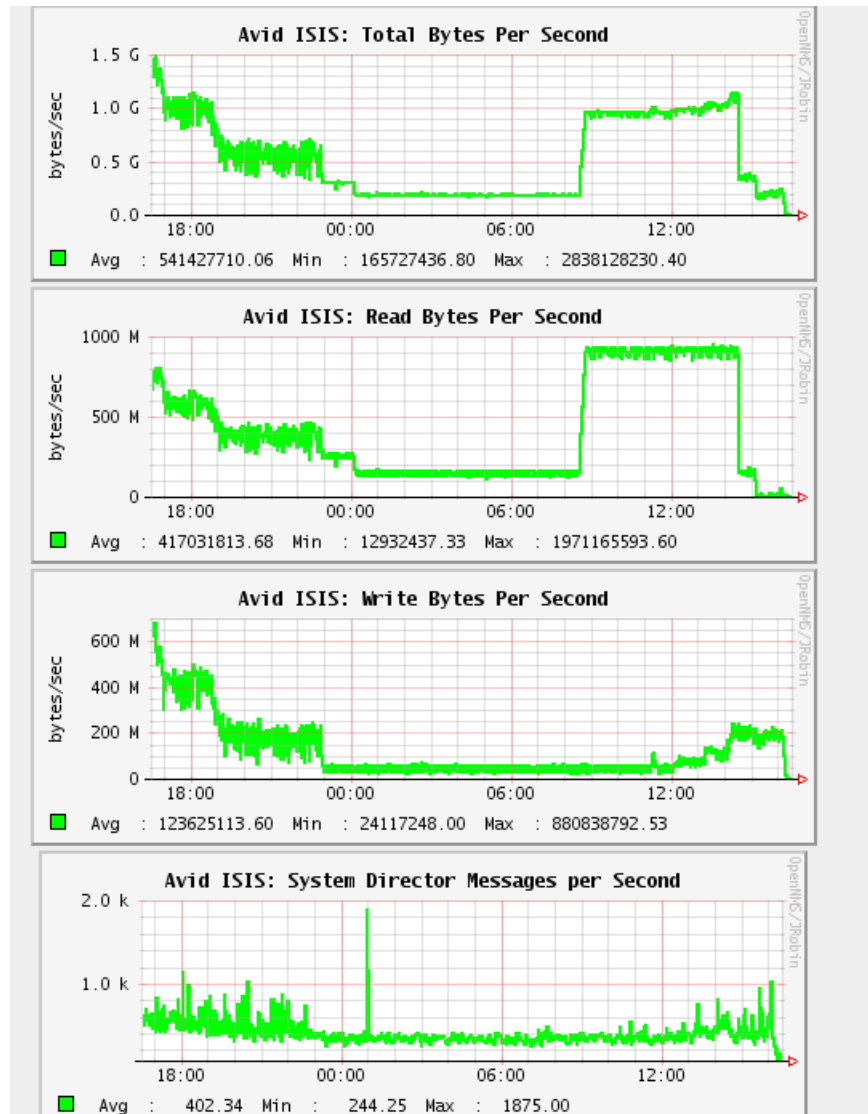
Drag Resources on the left to the bin on the right to graph

Nodes that support custom Avid monitoring features (Media Indexer, ISIS System Director, etc.) have a Node-Level Performance Data entry. The following example selects that as well as C:Label Boot (shows available local disk space), and Physical Memory.

- At the bottom of the Selected Resources to Graph panel, click Graph Selection. OpenNMS displays the Resource Graph page with the graphs you selected.



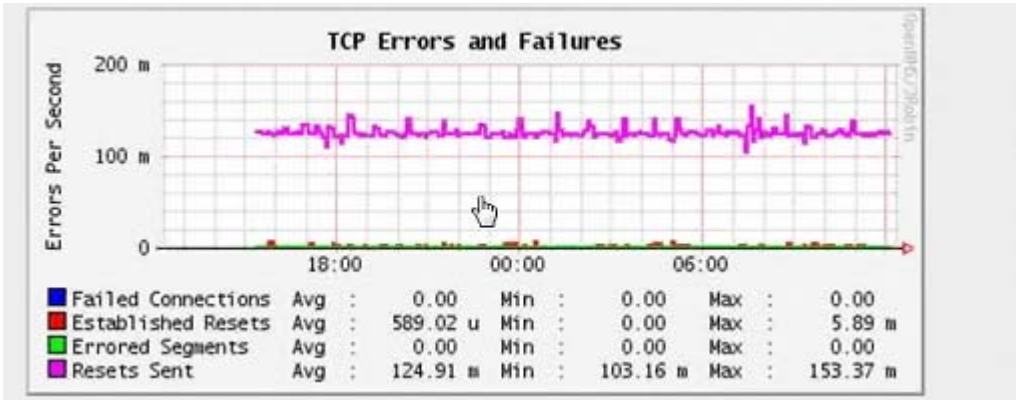
5. (Option) At the top of the display you can select from a number of options for graphs for the last week, month, or for a specific time period.
6. Scroll down to the graphs you are interested in. The following illustration shows several of the ISIS System Director graphs.



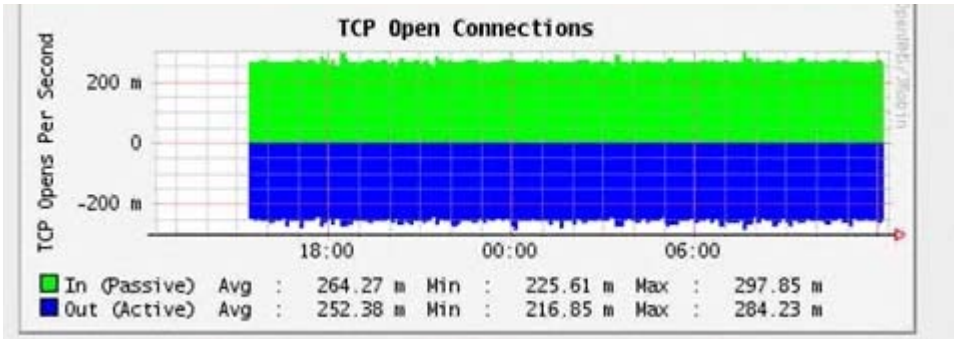
Notes About the Graphs

The following information relates to the graphs:

- A lowercase “m” on the left side of the graph denotes a fractional amount. For example, the TCP errors on the following graph represent a very small number of errors. Such a small amount as shown here is not cause for concern.



- Graphs scale to display the available data. Check the legend to determine whether the value is actually a large value or just a smaller value filling the available space, The following graph shows a scaled graph displaying small values.



- You can click on a graph to display it in a separate window. When displayed in a separate window, you can use the mouse to drag on portions of the graph and zoom in on a particular time period.

Creating Reports

OpenNMS has a feature known as KSC reports that allows you to display data from different nodes and different sources (snmp, icmp, http, etc.) on one page. For example, the following illustration shows a report for the number of unique media files and memory usage for two different Media Indexers.



Once you create the report you can generate it again at any time. This section describes how to create a KSC report.

To create a KSC report:

1. Select Reports from the OpenNMS top menu and click on “KSC Performance, Nodes, Domains.”

OpenNMS displays the Customized Reports page. The following illustration shows a system with three customized reports.

Customized Reports

Choose the custom report title to view or modify from the list below.
There are 3 custom reports to select from.

Reports
Force10 switch 10-ge bandwidth
ISIS bandwidth
Media Indexer - Unique Media Files

Page 1 of 1 | 1 - 3 of 3

☐ View
☐ Customize
☒ Create New
☐ Create New from Existing
☐ Delete

2. Select Create New and click Submit. The Customized Report Configuration window opens.

OpenNMS displays the Customized Report Configurations page.

Home / Reports / KSC Reports / Custom Report

Customized Report Configuration

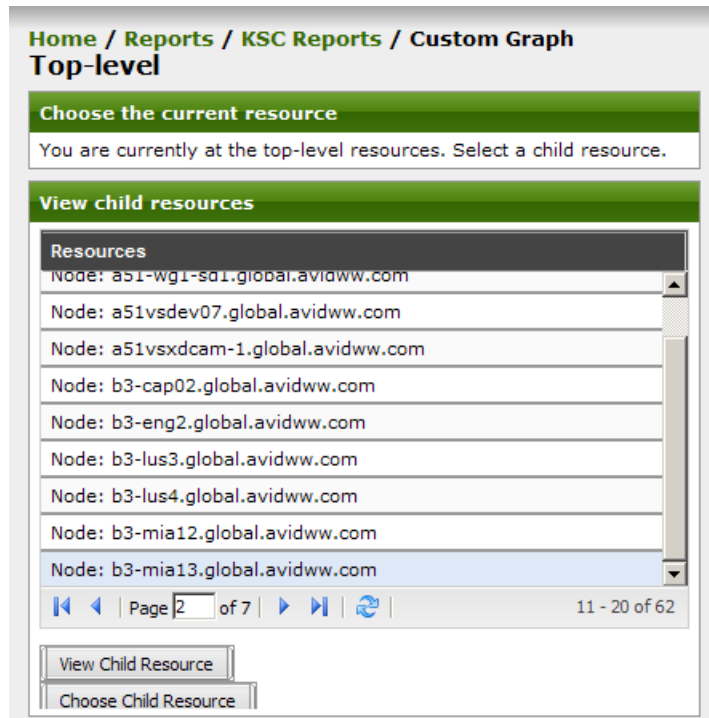
Title: Media Indexer Reports

☒ Show Timespan Button (allows global manipulation of report timespan)
☒ Show Graphtype Button (allows global manipulation of report prefabric

default Number of graphs to show per line in the report.

If you make any changes, please make sure to save the report when you are done.

3. Type a name for the report, select both check boxes, and click Add New Graph.
OpenNMS displays the “Choose the current resource” page and the View child resources dialog box.



4. Use the scroll bar and the page forward/backward buttons to locate the first node you want to appear in the report. This example selects a Media Indexer named b3-mia12.
5. Click View Child Resource.
OpenNMS displays the “View child resources” dialog box.

Home / Reports / KSC Reports / Custom Graph
Node: b3-mia12.global.avidww.com

Choose the current resource

This resource has no available prefabricated graphs. Select a child resource or the parent resource (if any).

View child resources

Resources
SNMP Node Data: Node-level Performance Data
SNMP Interface Data: Intel(R) PRO/1000 EB Network Connection...
SNMP Interface Data: Intel(R) PRO/1000 EB Network Connection...
Response Time: 10.104.100.6
Response Time: 10.104.108.6
Storage (MIB-2 Host Resources): C:\ Label:Boot Serial Number 1...
Storage (MIB-2 Host Resources): D:\ Label:Data Serial Number 6...
Storage (MIB-2 Host Resources): E:\
Storage (MIB-2 Host Resources): Physical Memory

Page 1 of 2 1 - 10 of 18

View Child Resource

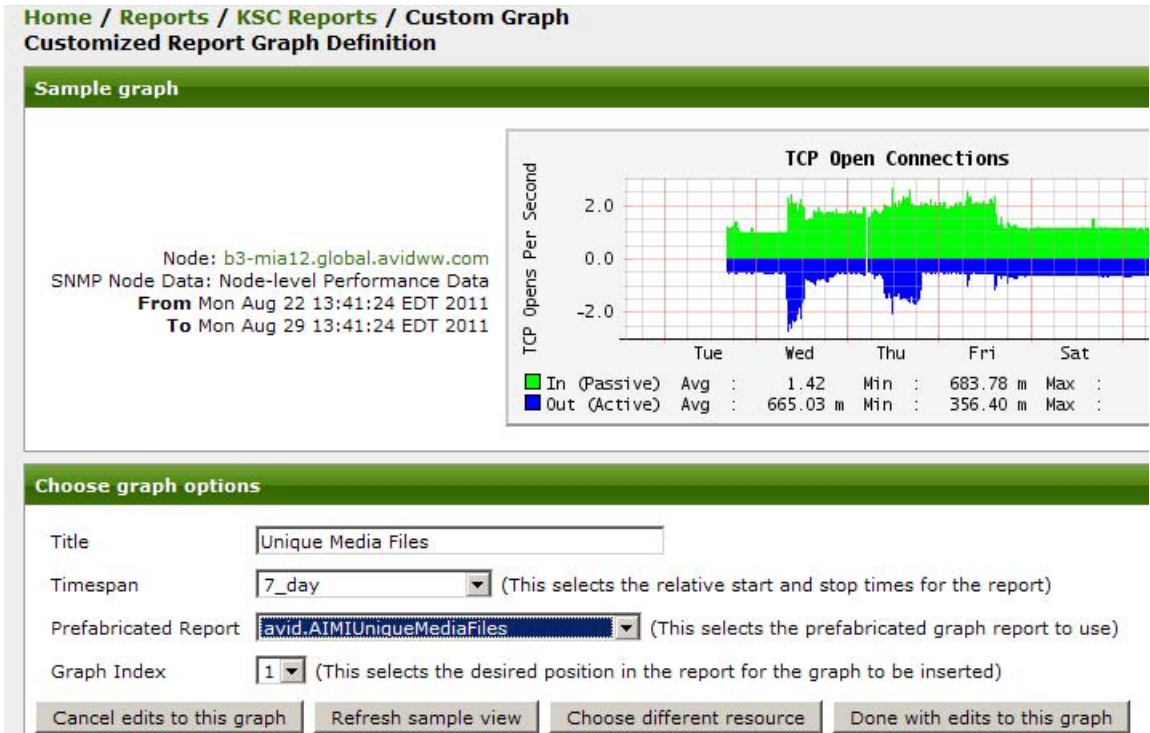
Choose Child Resource

Descriptions

The menu on the left can be any graph (e.g., response time), response time, etc.. These resources are then by child resource data, etc.. The resource you are viewing is the **current resource**. If the resource is the **current resource**, graph customization is available. If the current resource is a child resource, the "View child resources" link will be shown. The "View child resources" link can go straight to the child resource. The **View the parent** link will go to the parent resource. If the parent resource is a top-level resource, the "View the parent" link would be the top-level resource. If the parent resource is a child resource, the "View the parent" link would be the child resource. If the parent resource is a top-level resource, the "View the parent" link would be the top-level resource. If the parent resource is a child resource, the "View the parent" link would be the child resource.

6. Select the resource you want to graph and click "Choose Child Resource".

In this example, select "SNMP Node Data: Node Level Performance Data". That selection contains the custom Avid graphs that are available for a node. OpenNMS displays the "Choose graph options" dialog box.



7. Do the following:

- (Option) type a title for the graph
- Select a time span
- Select the option that you want to graph from the popup menu. Note that AIMI stands for Avid Interplay Media Indexer.
- Determine where the graph will appear in the list of graphs. When you add multiple graphs to a report this option is useful for rearranging the graphs.

8. Click “Done with edits to this graph.”

The following illustration shows the results after two graphs are added to the report. The graphs show the unique media files for two different Media Indexers.

Home / Reports / KSC Reports / Custom Report

Customized Report Configuration

Title:

Unique Media Files
Node: b3-mia13.global.avidww.com
SNMP Node Data: Node-level Performance Data

From: Mon Aug 22 13:42:38 EDT 2011
To: Mon Aug 29 13:42:38 EDT 2011

Avg : 2478698.86 Min : 2458389.42 Max : 2483

Unique Media Files
Node: b3-mia12.global.avidww.com
SNMP Node Data: Node-level Performance Data

From: Mon Aug 22 13:42:38 EDT 2011
To: Mon Aug 29 13:42:38 EDT 2011

Avg : 2477634.02 Min : 2234147.89 Max : 2483

☒ Show Timespan Button (allows global manipulation of report timespan)

☒ Show Graphtype Button (allows global manipulation of report prefabricated graph type)

Number of graphs to show per line in the report.

If you make any changes, please make sure to save the report when you are done. Changes will only be saved by using

9. Click Save. OpenNMS displays the report.



Its important to click Save on this page after you have added or modified graphs in the report. If you exit without clicking Save, your changes are lost.

10. At this point your add an additional graph, modify existing graphs, or rearrange the graphs in the report. Note that the line “Number of graphs to show per line in the report” allows you to add more than one graph per line as shown in the example at the beginning of this section.

Removing Discovered Services from a Node

This section describes how to remove services for a network switch. The same procedure can be used to remove services for any node.

For another example of removing a service, see [“Replacing the Service After You Configure the Provisioning Group” on page 97](#).

The Add Interface command forces an auto-discovery for the services on the node. For example, the following illustration shows the IP addresses of the switch and the two VLANs associated with the switch.

Availability		
Availability (last 24 hours)	99.104%	
172.20.54.38	Overall	97.313%
	HTTP	100.000%
	ICMP	100.000%
	InterplayEngine	91.940%
	Router	Not Monitored
	SNMP	Not Monitored
	StrafePing	Not Monitored
	Telnet	Not Monitored
172.20.108.1	Overall	100.000%
	HTTP	100.000%
	ICMP	100.000%
	InterplayEngine	100.000%
	Router	Not Monitored
	SNMP	Not Monitored
	StrafePing	Not Monitored
	Telnet	Not Monitored
172.20.108.65	Overall	100.000%
	HTTP	100.000%
	ICMP	100.000%
	InterplayEngine	100.000%
	Router	Not Monitored
	SNMP	Not Monitored

100% Acknowledged: (Check)

Recent Events			
☐	49895	3/25/09 16:47:00	Normal
☐	49891	3/25/09 16:46:54	Minor
☐	49415	3/25/09 15:46:08	Minor
☐	49414	3/25/09 15:46:00	Normal
☐	49413	3/25/09 15:46:00	Normal

Recent Outages	
Interface	Service
172.20.54.38	InterplayEngine

To remove extra discovered services from the OpenNMS display:

1. Click Admin and click Manage and Unmanage Interfaces and Services.

Home / Admin / Manage/Unmanage Interfaces

Manage and Unmanage Interfaces and Services

The two tables below represent each managed and unmanaged node, interface, and service combination. The 'Status' column means the interface or service is managed, and unchecked means not managed. Each different interface has a row listed below on light grey rows.

Managing or Unmanaging an interface will automatically mark each service on that interface as managed or unmanaged as well.

Apply Changes

Cancel

Select All

Unselect All

Reset

Status	Node Label	Interface	Service
☒	docisis.global.avidww.com	172.20.108.9	
☒	docisis.global.avidww.com	172.20.108.9	StrafePing
☒	docisis.global.avidww.com	172.20.108.73	
☒	docisis.global.avidww.com	172.20.108.73	StrafePing
☒	docmi.global.avidww.com	172.20.108.5	
☒	docmi.global.avidww.com	172.20.108.5	StrafePing

Status	Node Label	Interface	Service
☒	docisis.global.avidww.com	172.20.108.9	
☒	docisis.global.avidww.com	172.20.108.9	StrafePing
☒	docisis.global.avidww.com	172.20.108.73	
☒	docisis.global.avidww.com	172.20.108.73	StrafePing
☒	docmi.global.avidww.com	172.20.108.5	
☒	docmi.global.avidww.com	172.20.108.5	StrafePing

The window shows the services that are managed by all the nodes in the Node List.

2. Locate the node you are interested and uncheck the services you want to unmanage,

In this example we deselect the services for the two extra IP addresses and also deselect the InterplayEngine service.

☒	gw-isis-doc.global.avidww.com	172.20.54.38	ICMP
☐	gw-isis-doc.global.avidww.com	172.20.54.38	InterplayEngine
☐	gw-isis-doc.global.avidww.com	172.20.108.1	
☐	gw-isis-doc.global.avidww.com	172.20.108.1	HTTP
☐	gw-isis-doc.global.avidww.com	172.20.108.1	ICMP
☐	gw-isis-doc.global.avidww.com	172.20.108.1	InterplayEngine
☐	gw-isis-doc.global.avidww.com	172.20.108.65	
☐	gw-isis-doc.global.avidww.com	172.20.108.65	HTTP
☐	gw-isis-doc.global.avidww.com	172.20.108.65	ICMP
☐	gw-isis-doc.global.avidww.com	172.20.108.65	InterplayEngine

- Click Apply Changes and return to the Node List and select the switch.

The interface is now simplified for the switch.

Home / Search / Node
Node: gw-isis-doc.global.avidww.com
[View Events](#) [View Alarms](#) [Asset Info](#) [Telnet](#) [HTTP](#) [Resource Graphs](#) [Rescan](#) [Admin](#) [Update SNMP](#)

General (Status: Active)		
View Node Link Detailed Info		

Availability		
Availability (last 24 hours)	100.000%	
172.20.54.38	Overall	100.000%
	HTTP	100.000%
	ICMP	100.000%
	InterplayEngine	Rescan to Suspend
	Router	Not Monitored
	SNMP	Not Monitored
	StrafePing	Not Monitored
	Telnet	Not Monitored
172.20.108.1	Forced Unmanaged	
172.20.108.65	Forced Unmanaged	

Notification			
You: Outstanding: (Check)			
You: Acknowledged: (Check)			

Recent Events			
☐	52203	3/25/09 17:50:51	Warnin
☐	52202	3/25/09 17:50:51	Warnin
☐	52201	3/25/09 17:50:51	Warnin
☐	52200	3/25/09 17:50:51	Warnin
☐	52199	3/25/09 17:50:51	Warnin

[Acknowledge](#) [Reset](#) [More...](#)

Recent Outages	
----------------	--

Working with Alarms

You can define any event to also generate an alarm. By default many events have alarms associated with them but the System administrator can add or turn off the alarm association with particular events. Alarms allow you to view what you consider the most important events, usually on one page. They have the following benefits:

- You can view only those events that actually represent problems
- You can see how many of each of these have been received
- You or someone in your organization can acknowledge the event and take ownership of it
- If you use Acknowledgements in your monitoring workflow, you can specify that if a particular alarm is not acknowledged within a certain time period, it can be escalated to a critical alarm which causes a ticket event. You can configure ticket events to generate emails.

To view Alarms:

1. Click Alarms on the top menu bar. The system displays the Alarms window.
2. Click “All alarms (summary)”.

The system displays a summary of all alarms.

Home / Alarms / List
View all alarms Advanced Search Long Listing Severity Legend Acknowledge entire search

Alarm Text: Time: Any

Results: (1-6 of 6)
Search constraints: alarm is outstanding [-]

Ack	ID Severity	Node	Count	Last Event Time	Log Msg
☐	509		1	10/27/09 10:29:31 [<] [>]	OpenNMS user admin
☐	507	warrm-ipe1.avid-warroom.com [+] [-]	2	10/27/09 08:57:23 [<] [>]	InterplayEngine monit
☐	475	warrm-sswe.avid-warroom.com [+] [-]	1	10/25/09 12:20:21 [<] [>]	AvidClockVerification c Time difference betwe configured tolerance. [702918)/Ports:...
☐	474	warrm-sswe.avid-warroom.com [+] [-]	1	10/25/09 12:20:21 [<] [>]	AvidClockVerification c Time difference betwe configured tolerance. [702918)/Ports:...
☐	466		1	10/25/09 07:00:37 [<] [>]	OpenNMS user 'admin' failure event is BadCre
☐	379	warrm-ipe1.avid-warroom.com [+] [-]	13	10/27/09 08:57:23 [<] [>]	InterplayEngine datab

6 alarms Acknowledge Alarms

The following table describes the main items in the Alarms List window.

Item	Description
Ack check boxes	Allows you to acknowledge one or more alarms.
ID Severity	The ID for the alarm. Click the ID to see details.
Node	The node that generated the alarm. Click to get details on the node.
Count	The number of times this alarm has occurred.
Last Event Time	The last time this alarm occurred.

Item	Description
Log Msg	The main text associated with the Alarm. Click the ID Severity value for additional information.
Acknowledge Alarms menu	Allows you to select between the following: • Acknowledge Alarms • Clear Alarms • Escalate Alarms

The following illustration shows a close-up of the alarm message text for this example.

	Log Msg
[>]	OpenNMS user admin has logged in from 172.20.21.188.
[>]	InterplayEngine monitoring account is unable to login on interface 172.20.100.9
[>]	AvidClockVerification outage identified on interface 172.20.100.24 with reason code: Time difference between remote node and local clock reference exceeded the configured tolerance. [Configured Tolerance = 30000, Calculated difference = 702918]/Ports:...
[>]	AvidClockVerification outage identified on interface 172.20.101.24 with reason code: Time difference between remote node and local clock reference exceeded the configured tolerance. [Configured Tolerance = 30000, Calculated difference = 702918]/Ports:...
[>]	OpenNMS user 'admin' (may be blank) has failed to login from 172.20.21.188. The failure event is BadCredentialsException with the message 'Bad credentials'.
[>]	InterplayEngine database share unavailable on interface 172.20.100.9

The alarms in the above illustration are explained as follows:

- The first alarm indicates that an admin user has logged onto the Avid System Monitor. This alarm is green indicating that it is an informational event and no action is required.



For a description of the severity colors, click Severity Legend near the top of the Alarms List window or drag your cursor over the legend colors.

- The second alarm indicates that the Interplay Engine agent was unable to log onto the Interplay database. The agent performs this task periodically to ensure that the database is accessible.
- The AvidClockVerification alarms indicate that the Time Sync value used by the Avid System Monitor is more than the designated threshold for the two interfaces (nic cards) used by the node named warrm-sswe.avid-warrom.com. This could be a problem depending on the node. For example, editors may get Media Offline errors if the Media Indexer is losing ISIS notifications.
- The fourth alarm indicates that someone attempted to login as admin with the wrong password credentials.
- The final alarm indicates that the database share is not available to the Interplay Engine.

The second and final alarms indicate a problem on the Interplay Engine. In particular, the unavailable share event has occurred 12 times (see Count in the first illustration).

To find out detailed information about an alarm:

- Click the ID Severity button.

The following illustration shows the details for the Interplay login error.

Home / Events / Detail

Event 112956

Severity	Critical	Node	IE node2 ab6
Time	4/23/10 9:29:41 AM	Interface	172.20.107.16
Service	SNMP		
UEI	uei.opennms.org/avid/interplayengine/ieLoginCritical		

Log Message

InterplayEngine: login is currently not possible. The SNMP user cannot log on.

Description

Monitoring test account is not able to login.

Operator Instructions

The monitoring system periodically tries to logon to the Interplay Engine with a test user. The log Interplay Access and try to login with a regular user. If this does not work, see other monitoring further analysis.

[Acknowledge](#)

To find out additional information on the node generating the alarm:

- Click the Node name either on the Alarm List page or on the Alarm Details page.
- The following illustration shows the details for the Interplay Engine in this example.

graphs Rescan Admin Update SNMP

Notification

You: Outstanding: (Check)
You: Acknowledged: (Check)

Recent Events

☐	149932	10/27/09 08:57:23	Critical	InterplayEngine health status changed to critical condition on interface 172.20.100.8
☐	149931	10/27/09 08:57:23	Critical	InterplayEngine monitoring account is unable to login on interface 172.20.100.8
☐	149930	10/27/09 08:57:23	Critical	InterplayEngine database share unavailable on interface 172.20.100.8
☐	149929	10/27/09 08:57:23	Critical	InterplayEngine reports offline cluster group(s) on interface 172.20.100.8
☐	123231	10/24/09 08:56:53	Critical	InterplayEngine database share unavailable on interface 172.20.100.8

Acknowledge

Reset

More...

The Recent Events section of the Interplay Engine node page shows that there are some serious issues with this node that should be addressed.

In this case the Interplay Engine only needed to be restarted. The following illustration shows some of the events as the system was restarted and came back online.

10/27/09 13:33:46 [<] [>]	warrm-ipe1.avid-warroom.com	172.20.101.8 [+] [
uei.opennms.org/nodes/nodeRegainedService [+] [-] Edit notifications for event		
The Win32ClusterService outage on interface 172.20.101.8 has been cleared. Service is restored.		
10/27/09 13:33:42 [<] [>]	warrm-ipe1.avid-warroom.com	172.20.101.8 [+] [
uei.opennms.org/nodes/nodeRegainedService [+] [-] Edit notifications for event		
The SNMP outage on interface 172.20.101.8 has been cleared. Service is restored.		

10/27/09 13:33:24 [<] [>]	warrm-ipe1.avid-warroom.com	
uei.opennms.org/nodes/nodeUp [+] [-] Edit notifications for event		
Node warrm-ipe1.avid-warroom.com is up.		
10/27/09 13:33:11 [<] [>]	warrm-ipe1.avid-warroom.com	172.20.101.8 [+] [
uei.opennms.org/generic/traps/SNMP_Cold_Start [+] [-] Edit notifications for event		
Agent Up with Possible Changes (coldStart Trap) enterprise:.1.3.6.1.4.1.311.1.1.3.1.2 (.1.3.6.1.4.1.		
10/27/09 13:31:34 [<] [>]	warrm-ipe1.avid-warroom.com	172.20.100.8 [+] [
uei.opennms.org/nodes/dataCollectionFailed [+] [-] Edit notifications for event		
SNMP data collection on interface 172.20.100.8 failed.		

Acknowledging Alarms

Alarm notification provides an optional method of keeping track of when alarms are addressed by personnel at your site. Alarms can be acknowledged, or removed from the default view of all users, by selecting the alarms' Ack check box and clicking the Acknowledge Selected Alarms at the bottom of the page. Acknowledging an alarm gives users the ability to take personal responsibility for addressing a network or systems-related issue.

Any alarm that has not been acknowledged is active in the default alarms view of all users' browsers and is considered outstanding. Once you resolve the issue you can clear the alarm. The alarm remains in the system but the severity is changed to Cleared and the color is light green in the Alarm list.

The Details view of an alarm shows the user name of the person who acknowledged the alarm as shown in the following illustration. To view the details, click the ID Severity number for the alarm.

Node	warrm-ipe1.avid-warroom.com	Acknowledged By	admin
Interface	172.20.100.8	Time Acknowledged	10/27/09 5:12
Service	SNMP	Ticket ID	
UEI	uei.opennms.org/avid/interplayengine/ieLogin	Ticket State	

erplayengine/ieLogin:WARRM-NMS::

le to login on interface 172.20.100.9

n anymore on named host

lly login to engine failed. Open Interplay Access and try to login with a user. If it fails a serious problem exist. See additional

To acknowledge an alarm:

1. Click Alarms at the top of the OpenNMS window and then click All Alarms (summary).
2. Click the Ack check box associated with the alarm and click Acknowledge Selected Alarms at the bottom of the window.

The system removes the Alarm from view. Note that the alarm is removed from the view of all users.

Ack check box

Home / Alarms / List

View all alarms Advanced Search Long Listing Severity Legend Acknowledge entire search

Alarm Text: Time:

Results: (1-4 of 4)

Search constraints:

Ack	ID Severity	Node	Count	Last Event Time	Log N
☐	611	warrm-dms.avid-warroom.com [+] [-]	1	10/29/09 23:37:24 [<] [>]	AvidC Time config 30034
☐	610	warrm-gps.avid-warroom.com [+] [-]	1	10/29/09 23:34:09 [<] [>]	AvidC Time config 30252
☐	607	warrm-capman.avid-warroom.com [+] [-]	6	10/30/09 07:39:58 [<] [>]	SNMP
☐	606	warrm-capman.avid-warroom.com [+] [-]	1	10/29/09 15:15:58 [<] [>]	Node

4 alarms

Results: (1-4 of 4)

To view acknowledged alarms:

1. In the Alarms > List view, click the minus sign “[-]” in the Search constraints area.
The search constraints area changes to “alarm is acknowledged [-]” and the system displays the acknowledged alarms.

Click to view
acknowledged
alarms

Home / Alarms / List
View all alarms Advanced Search Long Listing Severity Legend Acknowledge entire search

Alarm Text: Time:

Results: (1-4 of 4)
Search constraints: alarm is outstanding [-]

Ack	ID Severity	Node	Count	Last Event Time	Log
☐	611	warrm-dms.avid-warroom.com [+] [-]	1	10/29/09 23:37:24 [<] [>]	AvidC Time config 3003:
☐	610	warrm-gps.avid-warroom.com [+] [-]	1	10/29/09 23:34:09 [<] [>]	AvidC Time config 3025:
☐	607	warrm-capman.avid-warroom.com [+] [-]	6	10/30/09 07:39:58 [<] [>]	SNMP
☐	606	warrm-capman.avid-warroom.com [+] [-]	1	10/29/09 15:15:58 [<] [>]	Node

4 alarms Acknowledge Alarms

Results: (1-4 of 4)

The system displays the acknowledged alarms as shown in the following illustration.

Home / Alarms / List
 View all alarms Advanced Search Long Listing Severity Legend Unacknowledge entire search

Alarm Text: Time:

Results: (1-12 of 12)
 Search constraints: alarm is acknowledged [-]

UnAck	ID Severity	Node	Count	Last Event Time	Log Msg
☐	553		26	10/30/09 09:01:28 [<] [>]	OpenNMS user admin h
☐	552		4	10/27/09 15:10:34 [<] [>]	OpenNMS user 'test_us The failure event is Ba
☐	507	warm-ipe1.avid-warroom.com [+] [-]	2	10/27/09 08:57:23 [<] [>]	InterplayEngine monito
☐	475	warm-sswe.avid-warroom.com [+] [-]	1	10/25/09 12:20:21 [<] [>]	AvidClockVerification o Time difference between configured tolerance. [1 702918)/Ports:...
☐	474	warm-sswe.avid-warroom.com [+] [-]	1	10/25/09 12:20:21 [<] [>]	AvidClockVerification o Time difference between configured tolerance. [1 702918)/Ports:...

To Clear an alarm:

1. Click the check box associated with the alarm and select Clear from the menu at the bottom of the window.
2. Click Go

The system changes the Severity of the alarm to Cleared and the changes the overall color to light green in the list.

Clearing an alarm allows you to show that an alarm has been both acknowledged and resolved.

To search for an alarm:

- ▶ To search for an alarm based on the alarm text, type the text in the Alarm Text box at the top of the Alarms list and click search.
- ▶ To search for an alarm based on the ID Severity, Click Admin > Alarms, enter the ID, and click Get Details.
- ▶ For the complete search criteria, click Admin > Alarms, and then click Advanced Search.

Running the Avid System Monitor Upgrade Utility

The upgrade utility allows you to upgrade an Avid System Monitor v1.1.1 or 1.2.0 installation to v1.2.1 while maintaining many of the customizations that you have made such as naming nodes and adjusting threshold values. The v1.2.1.580 upgrade tool upgrades any of the following builds to v1.2.1.580 (released version):

- v1.1.1.440 (v1.1.1 release)
- v1.1.1.445
- v1.2.0.525 (limited v1.2.0 release)
- v1.2.1.575 (v1.2.1 Beta release)

To view the version number of your Avid System Monitor software, see `opennms_config/etc/version.txt` on the installer or `OpenNMS/etc/version.txt` on an installed system. Each new release will have an updated upgrade utility. See the Avid System Monitor ReadMe on the Knowledge Base for details on the latest version.



Use the Upgrade Utility to upgrade an installation on the same server. Upgrading and moving to a different server at the same time is not supported.

As part of the upgrade process you will install OpenNMS v1.8.10. Note that the version of PostgreSQL does not change for this release.

To upgrade the OpenNMS configuration files:

1. Back up the Avid System Monitor files and the PostgreSQL database as described in [“To Perform a Complete Backup of Avid System Monitor” on page 192.](#)
2. Verify the locations of the Java JDK, OpenNMS, and PostgreSQL directories. The following shows the default locations:
 - C:\Program Files\Java\jdk1.6.0_13
 - C:\Program Files\OpenNMS
 - C:\Program Files\PostgreSQL
3. Before running the tool, make sure "Java\jdk1.6.0_13\bin" is in the windows path. See [“Setting the Path Environment Variable for Java” on page 187.](#)
4. Stop the Avid System Monitor service before beginning the upgrade.
5. Unzip the ASM_UpgradeUtility.zip.
6. Open a command prompt window and navigate to the ASM_UpgradeUtility folder.
7. Execute the run.bat command to start the upgrade utility.
8. When prompted, select the OpenNMS path and click Next.

9. Click the Upgrade button to begin converting the files.
10. Follow the system prompts to complete the upgrade.

The upgraded files are stored in the following directory:

C:\OpennmsUpgrade\etc

To install OpenNMS v1.8.10 and replace the upgraded configuration files:

1. Backup the following folder:
Program Files\OpenNMS\share
2. Uninstall OpenNMS (check the checkbox “force the deletion...”).
3. Use the Avid System Monitor installer to install OpenNMS v1.8.10.
4. Click “Copy OpenNMS config files” in the Avid System Monitor installer.
5. After the installation is complete, copy the files from C:\OpennmsUpgrade\etc into {OpenNMS}\etc.
6. Copy the share folder (see step 1) back into the Program Files\OpenNMS directory.

Setting the Path Environment Variable for Java

Before running the Upgrade Utility, you must set the Path environment variable for the version of Java used by the Avid System Monitor. This ensures that the Upgrade Utility uses the correct version of Java.

To set the Java path for Windows 2003 Server and Windows 2008 Server:

1. Do one of the following:
 - For Windows 2003 Server: Click Start > Control Panel > System > Advanced.
 - For Windows 2008 Server: Right-click the My Computer icon, select Properties, and then click “Advanced system settings.”
2. Click Environment Variables.
3. Under System Variables, locate the PATH variable, and select it.
4. Click Edit.
5. In the Edit window, modify PATH by appending the Java JDK path. The following example shows the correct format using the default path:

C:\Program Files\Java\jdk1.6.0_13\bin;

If the PATH environment variable does not exist, add a new variable named PATH with the following value:

C:\Program Files\Java\jdk1.6.0_13\bin;



Make sure you use the correct path for your system. For example, the Java JDK may be installed on the D: drive.

6. Click OK.

Correcting Links to the OpenNMS Home Page After the Upgrade

If you have links to the OpenNMS home page, after the upgrade you may get a “page not found” error or an HTTP error when clicking on a link to the OpenNMS page. You can either edit the link to fix the problem.

To fix a link to the OpenNMS page after the upgrade:

1. Locate the link in your favorites or on your web page.
2. Remove the text “acegilogin.jsp” from the end of the link. For example, the following sample link may return an HTTP error after the upgrade:

`http://10.106.25.10:8980/opennms/acegilogin.jsp`

The following link should work correctly:

`http://10.106.25.10:8980/opennms/`

Modifying Provisioning Groups after the Upgrade

OpenNMS adds a number of default service monitoring items called detectors to each provisioning group. These detectors are not needed by Avid System Monitor and should be deleted from the provisioning groups that you use at your site. The following procedure describes how to delete the detectors. For additional information, see [“Changes to Provisioning Groups” on page 32](#).

To delete the detectors in a Provisioning Groups:

1. Click the Admin link in OpenNMS.
2. Under the Nodes section, click Manage Provisioning Groups.

The Provisioning Groups window opens. The following illustration shows the OpenNMS provisioning group page.

The screenshot shows the openNMS web interface. At the top is a navigation bar with links: Node List, Search, Outages, Path Outages, Dashboard, Events, Alarms, Notifications, Assets, and R. Below this is a breadcrumb trail: Home / Admin / Provisioning Groups. A search bar is followed by buttons: Add New Group, Edit Default Foreign Source, and Reset Default Foreign Source. The main content area has a green header for 'IPE-DualNIC'. Below it are buttons: Delete Group and Synchronize. The 'Synchronize' button is annotated with 'Synchronize button (formerly Import)'. To the right of the buttons is a table of provisioning groups. The first group is 'IPE-DualNIC', which is highlighted. It has an 'Edit' link annotated with 'Provisioning group edit button'. The table shows details for this group: 2 nodes defined, 0 nodes in database, Last Modified: 2011-06-02T13:55:28.265-04:00, and Last Synchronization Requested: 2009-06-15T15:13:45.484-04:00. Below the table is a section for 'IPE-SingleNIC' with buttons: Delete Nodes and Synchronize. The 'Edit' link for this group is annotated with 'Foreign Source Edit button'.

Annotations:

- Synchronize button (formerly Import)
- Provisioning group edit button
- Foreign Source Edit button

Page Content:

openNMS®

Node List Search Outages Path Outages Dashboard Events Alarms Notifications Assets R

Home / Admin / Provisioning Groups

Search Add New Group Edit Default Foreign Source Reset Default Foreign Source

IPE-DualNIC

Delete Group Synchronize

Requisition (Provisioning Group):
Define node and interface data for synchronization.

Foreign Source:
Define scanning behavior for synchronization.

Edit

2 nodes defined, 0 nodes in database
Last Modified: 2011-06-02T13:55:28.265-04:00
Last Synchronization Requested: 2009-06-15T15:13:45.484-04:00

Edit | Clone
Last Modified: Fri May 27 15:58:46 EDT 2011

IPE-SingleNIC

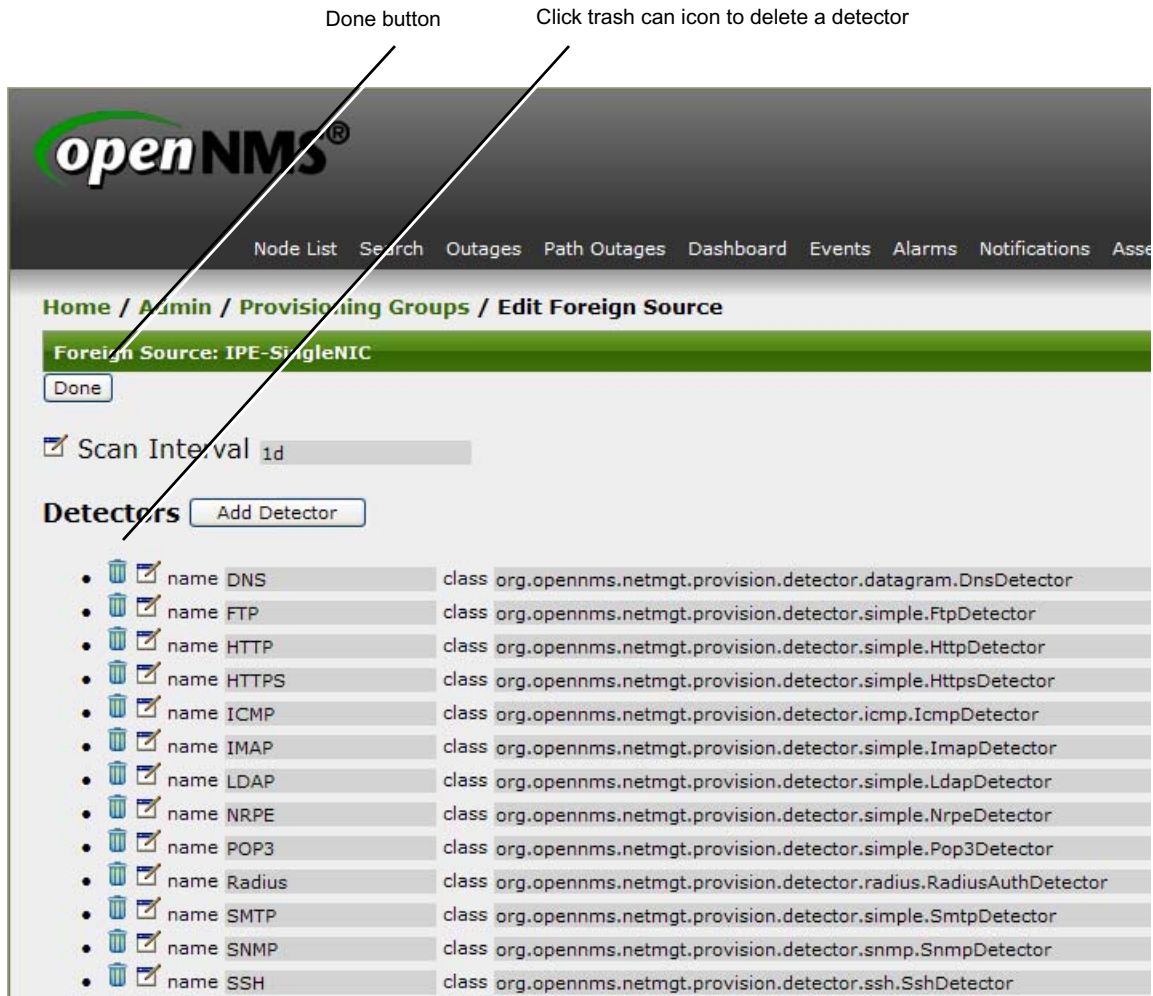
Delete Nodes Synchronize

Requisition (Provisioning Group):
Define node and interface data for synchronization.

Edit

3 nodes defined, 3 nodes in database

3. Locate the Provisioning Group you want to edit. For example, IPE-Dual-NIC.
4. (Option) Click the Provisioning group edit button and check that your settings are still available after the upgrade. Then click Done.
5. Click the Foreign Source Edit button. and delete all of the detectors on the page.



6. Click each trash can icon to delete all of the detectors on the page.
7. Click Done and then click Synchronize to load the changes to OpenNMS.

To re-create the OpenNMS Dashboard:

1. The upgrade utility does not bring the Avid System Monitor v1.1.1 Dashboard forward. You must re-create the Dashboard after the upgrade.
2. For information on configuring the dashboard, see [“Configuring the Dashboard” on page 113](#). As described in that section, you can copy text from the file `etc\surveillance-views.xml` when you are setting up the dashboard. It is important to use the file after the upgrade because several of the names of the rows and columns are different for this release from the ones described in the doc.

You can use the default names in the surveillance-views.xml file or change the names to match any custom values you use for your own dashboard. If you edit the values in the file, make sure you change both the label name and the category name (one above the other).

The following illustration shows the row and column names in the default v1.2.1 surveillance-views.xml file:

```
<views >
  <view name="default" refresh-seconds="300" >
    <rows>
      <row-def label="ISIS System Directors" >
        <category name="ISIS System Directors"/>
      </row-def>
      <row-def label="Ingest and Playout" >
        <category name="Ingest and Playout" />
      </row-def>
      <row-def label="Interplay Database Engines" >
        <category name="Interplay Database Engines" />
      </row-def>
      <row-def label="Interplay Services" >
        <category name="Interplay Services" />
      </row-def>
      <row-def label="Interplay Providers" >
        <category name="Interplay Providers" />
      </row-def>
      <row-def label="LAN Gateways" >
        <category name="LAN Gateways" />
      </row-def>
      <row-def label="Network Services - AD, DNS, DHCP" >
        <category name="Network Services - AD, DNS, DHCP" />
      </row-def>
    </rows>
    <columns>
      <column-def label="workgroup" >
        <category name="workgroup" />
      </column-def>
      <column-def label="Test Lab" >
        <category name="Test Lab" />
      </column-def>
      <column-def label="Future Use" >
        <category name="Future Use" />
      </column-def>
    </columns>
  </view> </views>
```

Backing Up and Restoring Avid System Monitor

This section describes how to backup and restore the PostgreSQL database as well as the OpenNMS configuration that contain the Avid customizations as well as any that you have added. Avid recommends that you periodically perform a backup and save the backup on a separate computer. Its also recommended that you perform a backup before you upgrade Avid System Monitor to a new version.

To Perform a Complete Backup of Avid System Monitor

This section describes the backup procedure.

To backup Avid System Monitor:

1. Stop the Avid System Monitor service.
2. Make copies of the following folders:
Program Files\OpenNMS\etc
Program Files\OpenNMS\share
3. Backup the PostgreSQL database as described in the following section.
4. (Option) Restart the Avid System Monitor service if you want to continue working with Avid System Monitor.

Backing Up and Restoring the PostgreSQL Database

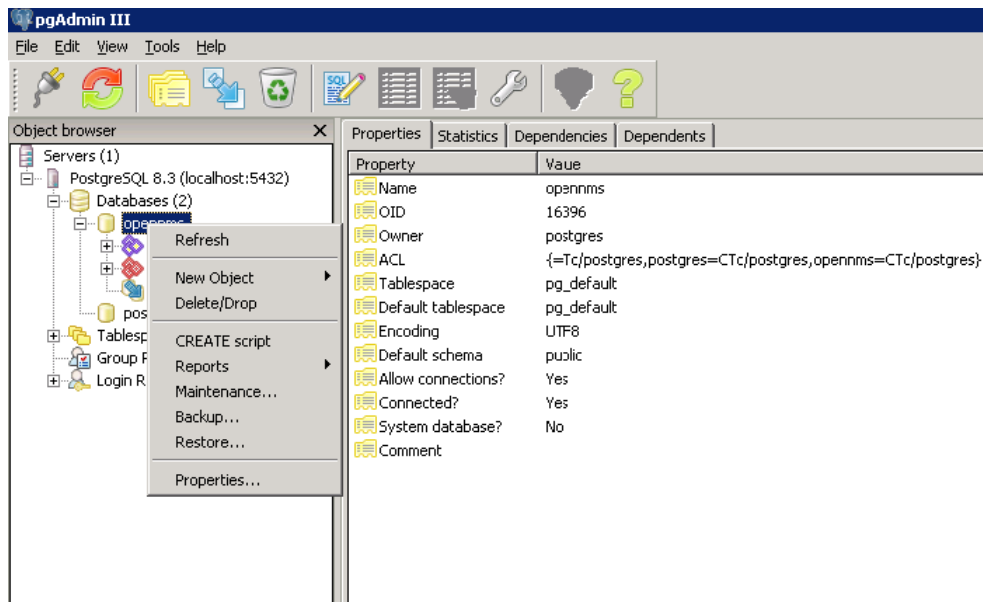
This section describes the PostgreSQL backup and restore procedures.

Backing Up the PostgreSQL Database

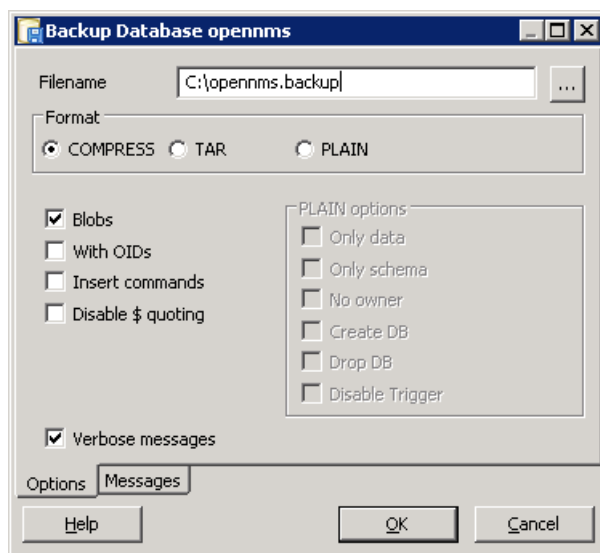
This procedure describes how to back up the database.

To backup the PostgreSQL database:

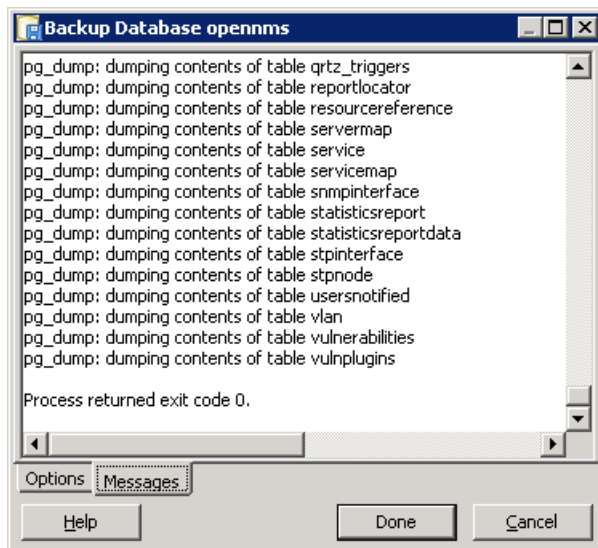
1. Select Start > All Programs > PostgreSQL > pgAdmin III.
2. Right-click the opennms database and select Backup.



3. In the “Backup Database opennms” dialog, enter a name for the file, browse to a target location and leave all other options as default.



4. Click OK A progress dialog box opens as shown in the following illustration.



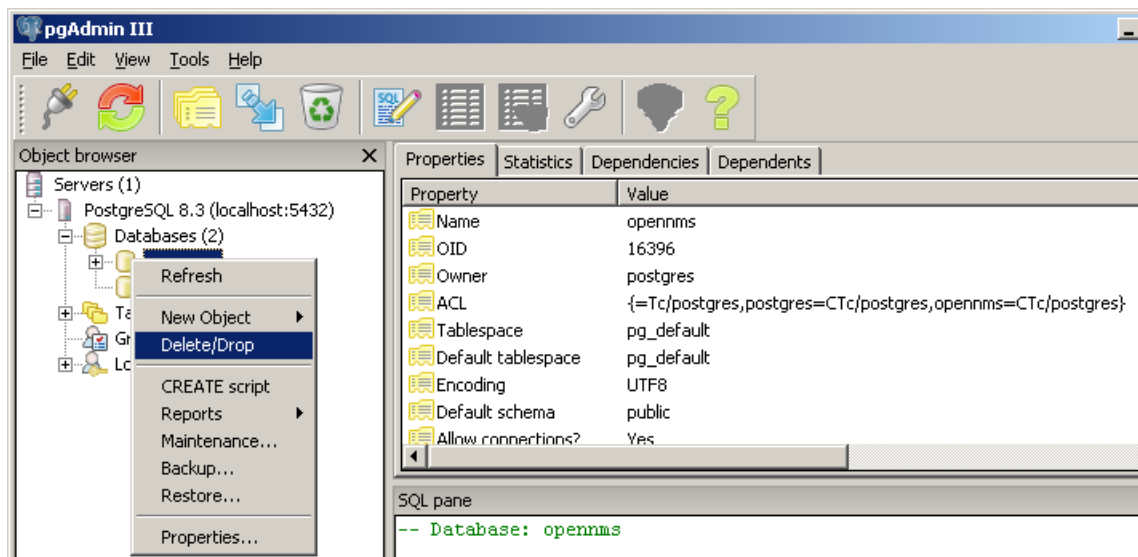
5. Click Done when the backup operation is complete.

Restoring the PostgreSQL Database

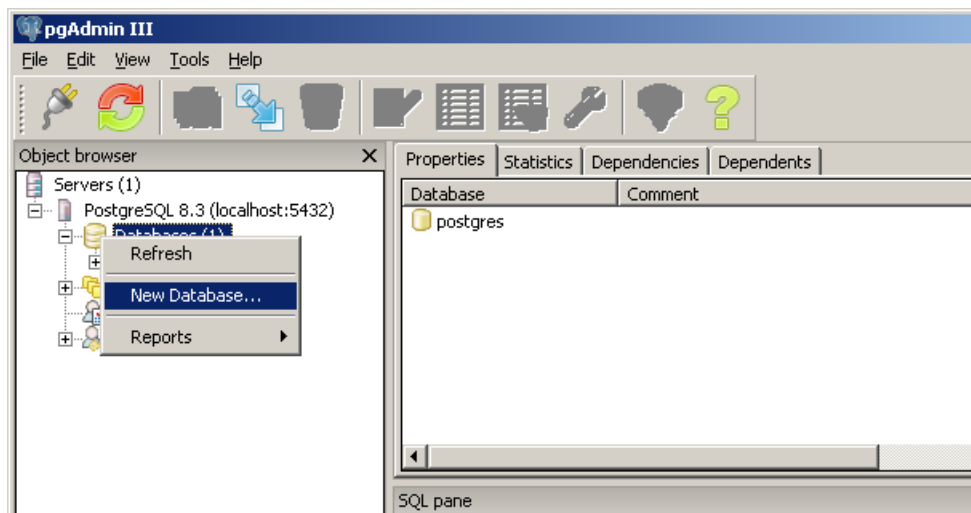
This procedure describes how to restore the database.

To restore the PostgreSQL database:

1. Select Start > All Programs > PostgreSQL > pgAdmin III.
2. Right-click the opennms database and select Delete/Drop.



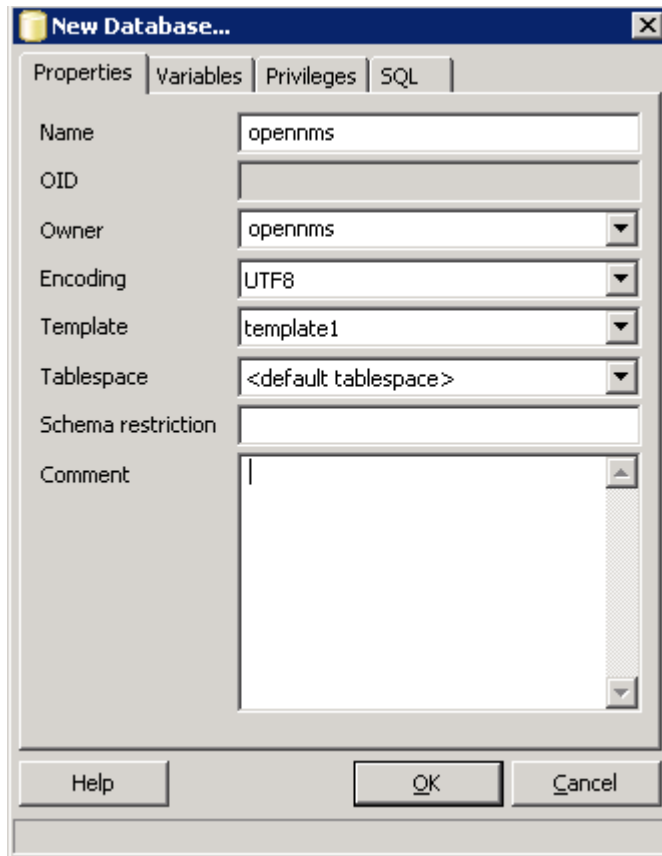
3. Right-click the Database icon and select New Database.



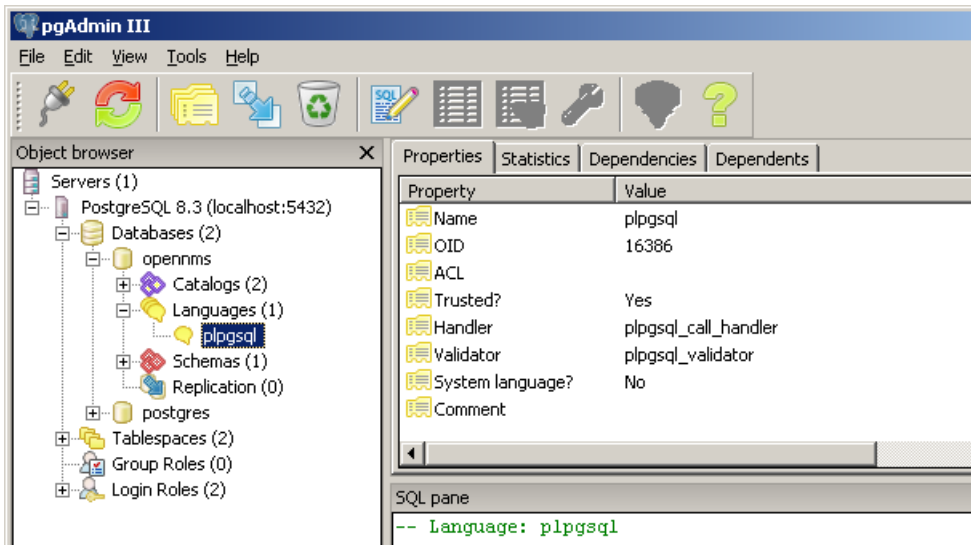
4. In the New Database dialog, select or enter the following options:

- owner: opennms
- encoding: UTF-8
- template: template1

Use the default values for all other options as shown in the following illustration.

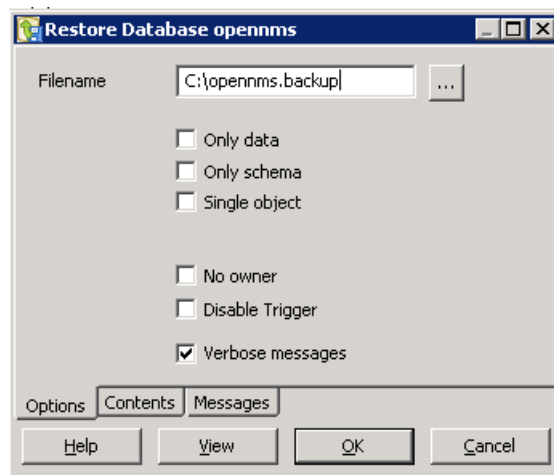


5. Click OK.
6. After PostgreSQL creates the opennms database, click the database to expand it in the object browser.
7. Locate the plpgsql languages, right click the entry, and delete it.

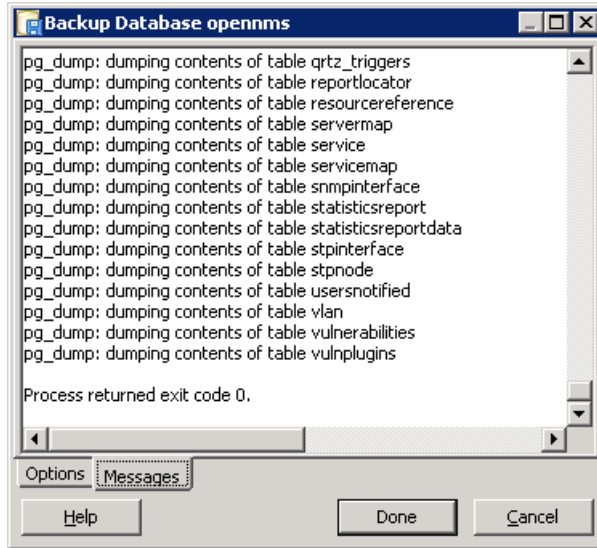


 *If the Languages option is not available, select File > Options > Display tab and select the Languages option.*

8. Right-click the opennms database and select Restore.
9. In the Restore Database dialog, browse to the location of the backup file and select the file. Leave all other options as default.



10. Click OK and then click Done when the backup operation is complete.



Restoring an Avid System Monitor Backup

This section describes how to restore the PostgreSQL database and the OpenNMS backup files. It involves the following operations:

- Uninstall Java, PostgreSQL, and OpenNMS and delete the application folders
- Reinstall the same versions of Java, PostgreSQL, and OpenNMS
- Restore the backed up PostgreSQL database and the backed up OpenNMS files.



This restore operation is qualified for a restoration on the same computer or on a different computer with the same operating system. It is not qualified for moving between different operating systems because of the change in path names that can exist on a different OS.

To restore Avid System Monitor from a backup:

1. Stop the Avid System Monitor service.:
2. Make note of whether the Java, OpenNMS, and PostgreSQL installations are on the C drive or the D: drive. You must install to the same drives later in the procedure to maintain the directory paths.
3. Uninstall OpenNMS (check the box to delete OpenNMS files).
4. Uninstall PostgreSQL using Add/Remove Programs.
5. Uninstall Java.

6. Reboot.
7. Delete the remaining Java, Postgres, OpenNMS directories.



Its important to delete the folders at this step.

8. Install Java, Postgres, OpenNMS (the same versions you backed up). Install all three on the same drive (C: or D:) as before.
9. Reboot.
10. Stop the Avid System Monitor service.
11. Restore the PostgreSQL database. See [“Restoring the PostgreSQL Database” on page 194.](#)
12. Copy the /etc and /share directories from your backup to OpenNMS (overwrite the existing files).
13. Reboot.

